
K
GUÍA DE VIAJE
AL MUNDO DIGITAL
POLÍTICAS DE CIBERSEGURIDAD
PARA PERSONAS DEFENSORAS DE
LOS DERECHOS HUMANOS

Fundación Karisma

Esta publicación es una traducción, adaptación y actualización de *Travel Guide to the Digital World: Cybersecurity Policy for Human Rights Defenders* publicada por Global Partners Digital.

Esta publicación fue realizada por la Fundación Karisma con el apoyo y financiación de Global Partners Digital.



ADAPTACIÓN Y ACTUALIZACIÓN
Amalia Toledo

TRADUCCIÓN
Mateo Reyes
frontera.traduccion@gmail.com

REVISIÓN
Carolina Botero
Juan Diego Castañeda
Stephane Labarthe

DISEÑO EDITORIAL E ILUSTRACIONES
Sergio García Casas
Mapa pag. 49 - Hugo A. Vásquez

ABRIL DE 2020









En los últimos años, puede que hayan notado el aumento de la prominencia de un cierto prefijo.

Historias escabrosas de “cibercrímenes” y “cibercriminales” abundan en los medios de comunicación. El “ciberacoso” y el “ciberma-toneo” son problemas sociales ampliamente reconocidos. En anticipación a las “cibera-menazas” o al “ciberterrorismo”, los Estados realizan “ciberejercicios” y firman “ciberpac-tos” o “ciberacuerdos” de alto perfil con otros Estados. Un dominio en rápida expansión de la “ciberley” trata de mantenerse al día con todo.

Lo curioso del prefijo “ciber” es que cuanto más se usa, menos significado parece tener. Lo “ciber” puede encapsular todo y nada al mismo tiempo. Para localizar las razones de esta elas-ticidad, podría ser útil una breve mirada a la historia de la palabra.

La historia comienza con la antigua palabra grie-ga “kubernesis”, que significa dirección, control o gobierno. Varios miles de años más tarde, en 1940, un matemático estadounidense, Norbert Wiener, acuñó la palabra “cibernética” para des-cribir el emergente campo de la robótica.

En 1982, se produce una mutación significativa. En un cuento corto, el escritor de ciencia ficción William Gibson inventó una nueva palabra, “ciberespacio”, para describir un reino abstracto e ingobernable. Aquí, crucialmente, la connotación es anárquica, no de control. La palabra se convirtió rápidamente en sinónimo del emergente entorno digital; su prefijo es un medio de llevar los fenómenos fuera de línea a un contexto en línea.

Hoy en día lo “ciber” ha cerrado el círculo en algunos aspectos. El espacio ingobernable evocado por Gibson ha desaparecido. El ciberespacio es ahora indiscutiblemente una zona de contención para los Estados, sujeta a control y gobernanza cada vez mayores. Nuevas palabras como ciberguerra, ciberdelin-cuencia y ciberseguridad llevan consigo la noción de categorizar y gobernar el número de actores, espacios y prácticas que existen en el universo digital.

En medio de todo esto, es la palabra “ciberseguridad” la que se ha converti-do en la más dominante. Es un objetivo que los gobiernos invocan y per-siguen incansablemente a través de la política. Se utiliza para referirse a cualquier cosa, desde los programas de alfabetización digital hasta las leyes con nuevos y amplios poderes de vigilancia.

¿Qué es exactamente la ciberseguridad y por qué la elaboración de políticas de ciberseguridad debería importar a las personas defensores de los derechos humanos?

SOBRE ESTA GUÍA 8

CAPÍTULO 1
ENTENDAMOS LA CIBERSEGURIDAD 12
Definir la ciberseguridad 13
¿Qué sucede si no hay ciberseguridad? 16
Dimensiones de la política de ciberseguridad 18
Actores de la ciberseguridad y sus desafíos 19
¿Cómo se relacionan los derechos humanos con la ciberseguridad? 33
¿Cómo sería un ciberespacio basado en los derechos humanos? 40

CAPÍTULO 2
LA CIBERSEGURIDAD COMO SEGURIDAD DE LA INFORMACIÓN 42
Normas técnicas internacionales 45
Obligaciones y responsabilidades legales 48
Prácticas de intercambio de información 50
Capacidad de gestión, respuesta y coordinación de incidentes: CERT y CSIRT 54
Incorporar derechos humanos a las políticas sobre seguridad de la información 56

CAPÍTULO 3
LA CIBERSEGURIDAD COMO CIBERDELITO 62
El propósito de las leyes contra el ciberdelito 65
Vigilancia masiva 74
Cifrado 82
Uso del anonimato en internet 88
Restricciones y cortes de internet 92
Incorporar derechos humanos a la formulación de políticas sobre ciberdelitos 95

CAPÍTULO 4
LA CIBERSEGURIDAD COMO CIBERCONFLICTO 100
Principales prioridades y debates de política pública 102
Incorporar derechos humanos a la formulación de políticas sobre ciberconflictos 112

PRINCIPIOS PARA LA PARTICIPACIÓN EN LA POLÍTICA DE CIBERSEGURIDAD 114

GLOSARIO 120

RECURSOS SELECCIONADOS 132



SOBRE ESTA GUÍA

Las personas defensoras de derechos humanos desempeñan un papel fundamental para garantizar que las políticas gubernamentales se ajusten a las normas de derechos humanos establecidas. Cuando están ausentes de la formulación de políticas, existe el riesgo de que las decisiones políticas importantes se vean impulsadas por ganancias políticas a corto plazo, y no por la promoción y protección de los derechos humanos. La capacidad de las personas defensoras de derechos humanos para contribuir a la política pública y examinarla depende de que tengan un nivel básico de conocimiento de las instituciones, los interesados y las cuestiones pertinentes en juego.

Cuando se trata de la ciberseguridad, es cada vez más evidente que las personas defensoras de derechos humanos no tienen, en general, ni capacidades para involucrarse en la construcción de políticas públicas sobre este asunto. Dependiendo de con quién se hable y en qué foro, la ciberseguridad puede extenderse a cuestiones tan diversas como los protocolos de seguridad en las bases de datos gubernamentales y las normas internacionales aplicables a los **ciberataques** durante los conflictos armados.

A nivel fundamental, las personas defensoras de derechos humanos también se ven obstaculizadas por la falta de un lenguaje acordado con el que debatir la ciberseguridad. Muchos de los conceptos en este ámbito como “ciberataque”, “seguridad de la información” o “ciberconflicto” tienen significados controvertidos, que son objeto de un debate continuo y, en algunos casos, de manipulación con fines políticos.

Esta guía tiene por objeto ayudar a corregir el desequilibrio en la capacidad y los conocimientos técnicos entre las personas defensoras de derechos humanos, y quienes son responsables de la formulación de políticas públicas o tienen alguna responsabilidad en el campo de la ciberseguridad.

En el corazón de esta guía se encuentra un intento de abordar quizás la barrera fundamental: la ausencia de definiciones claras y términos acordados. Para ello, examinamos detenidamente tres esferas distintas de política que a menudo se combinan bajo el paraguas de la ciberseguridad –seguridad de la información, ciberdelincuencia y ciberconflicto–, desentrañando sus dimensiones políticas y jurídicas, localizando a las partes interesadas relevantes y esbozando las cuestiones que están en juego. Esperamos que esto ayude a las personas defensoras de los derechos humanos a participar eficazmente en los debates de ciberpolítica en los planos nacional, regional e internacional.

El capítulo 1 abarca los fundamentos de la ciberseguridad: qué es, su relación con los derechos humanos y de dónde proceden las políticas. En el capítulo 2 se examinan las repercusiones en materia de derechos humanos de una serie de cuestiones relacionadas con la seguridad de la información, incluida la necesidad de normas técnicas internacionales sobre ciberseguridad y el intercambio de información sobre ciberamenazas. En el capítulo 3 se pone de relieve la legislación sobre el ciberdelito, se examina lo que regula y los tipos de medidas que incentiva, incluida la **vigilancia masiva**, las prohibiciones al **cifrado** y las medidas para socavar el **anonimato** en línea. En el capítulo 4, la guía se centra en los conflictos cibernéticos y en el debate en evolución sobre la aplicación de las normas de relaciones internacionales al ciberespacio. En cada sección, sugerimos formas en las que las personas defensoras de derechos humanos pueden incorporar los derechos humanos en los debates sobre políticas de ciberseguridad. Al final, proponemos algunos principios generales para incluir los derechos humanos en la formulación de políticas de ciberseguridad. Esta guía está dirigida a un público no técnico, por lo que también hemos añadido un glosario donde se explican las palabras en negrita.

Esta guía viene con una advertencia. La ciberseguridad es un área de la ley y la política que crece y cambia rápidamente. Sigue habiendo poco consenso, especialmente entre los gobiernos, sobre el alcance y la aplicación de la ciberseguridad, por no hablar de su relación con los derechos humanos. Por consiguiente, las opiniones expresadas aquí son las de un actor entre muchos, y la categorización de las cuestiones adoptadas aquí no es ni exhaustiva ni definitiva.

En este ámbito emergente, las personas defensoras de derechos humanos tendrán que hacer algo más que formular políticas. Tendrán que participar activamente en la configuración de la propia definición y misión de las políticas de ciberseguridad: lo que abarca, lo que significa, lo que incluye y lo que excluye. Si esta tarea se deja exclusivamente en manos de las personas profesionales de la seguridad y de los gobiernos, la probabilidad de que surjan políticas que refuercen la seguridad individual y defiendan los derechos humanos no será elevada.



1 ENTENDAMOS LA CIBERSEGURIDAD

¿De qué estamos hablando?
¿Cómo mantener la seguridad en línea?

DEFINIR LA CIBERSEGURIDAD

Una definición convencional de la ciberseguridad, como la que encontramos en las estrategias gubernamentales y en manuales corporativos, sostiene que la ciberseguridad se relaciona con la protección de la información que existe en el entorno digital contra la intrusión, adquisición o explotación no autorizada.

Sin embargo, la ciberseguridad ha adquirido un significado mucho más amplio. Los gobiernos, las instituciones, los medios de comunicación y la sociedad civil utilizan el término para referirse a una amplia gama de situaciones que se encuentran fuera de esta visión tradicional de la ciberseguridad. Tomemos los ejemplos a continuación, que podrían clasificarse como cuestiones de ciberseguridad:

Un ataque de ***phishing*** lleva a cientos de personas incautas a revelar su usuario y contraseña para acceder a su banco.

Una **vulnerabilidad** en un software permite acceder a las claves privadas de los servidores, y a las ***cookies*** y contraseñas de las personas usuarias.

Un sistema de información hospitalario afectado por un ataque hace imposible acceder a los datos de sus pacientes.

Un apagón causada por un ciberataque sumerge una ciudad en la oscuridad.

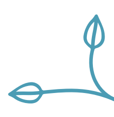
Una célula terrorista planea un ataque a través de una red oculta.

El suministro de agua de una ciudad se vuelve inseguro después de que un **ataque** permite el control remoto no autorizado de una planta de suministro de agua.

Un video que infringe derechos de autor se sube a un sitio web.

Una red de narcotraficantes usa criptomonedas para traficar narcóticos ilegales.

La publicación en redes sociales de un comentario insultante contra algún liderazgo político.



El término también se puede utilizar para justificar medidas que socavan los derechos humanos. Por ejemplo, a menudo los gobiernos utilizan la ciberseguridad para justificar restricciones a la navegación en internet, para controlar el uso de herramientas de anonimización y los servicios cifrados, y para expandir los poderes de vigilancia de los cuerpos policiales y de inteligencia (consulte la página 17 para obtener información más detallada sobre cómo las medidas políticas pueden socavar los derechos humanos).

A falta de definiciones acordadas sobre ciberseguridad, su significado dependerá mucho de quién lo haga. Algunos actos que se entenderían como discursos protegidos por la libertad de expresión en el sistema interamericano de derechos humanos (ej. insultar a un líder político) pueden clasificarse fácilmente como ciberdelitos debido a la ambigüedad de la definición. Entonces, quizás las preguntas más relevantes son ¿quién decide qué es la ciberseguridad y qué no lo es? y ¿dónde se toma esa decisión?

En comparación con otras políticas que pueden tener un impacto en los derechos humanos, la ciberseguridad plantea un desafío conceptual particular. En parte, esto se debe a la naturaleza misma de la "seguridad", que es imposible de alcanzar o perfeccionar por completo. Por esta razón, la ciberseguridad es una circunstancia que cambia constantemente y cuya realidad se puede moldear desde las políticas públicas.

TRABAJO DE LA *FREEDOM ONLINE COALITION* SOBRE UNA INTERNET LIBRE Y ABIERTA

El Grupo de Trabajo sobre una internet libre y abierta (consulte página 111) ha propuesto una definición de ciberseguridad que se centra en la seguridad de las personas, como también de los sistemas: "La ciberseguridad es la preservación – a través de políticas, tecnologías y educación – de la disponibilidad, confidencialidad e integridad de la información y su infraestructura subyacente, a fin de mejorar la seguridad de las personas, tanto en línea como fuera de línea"

La diversidad de actores implicados en la ciberseguridad también plantea desafíos. Este es un asunto para los actores gubernamentales, instituciones intergubernamentales, comunidades técnicas y académicas, el sector privado y la sociedad civil (consulte las páginas 19-32). A falta de una definición estable, el término se ha vuelto increíblemente amplio, refiriéndose a los fenómenos que van desde los **ciberataques** transfronterizos, pasando por el spam, hasta las normas técnicas de los sistemas de votación.

¿QUÉ SUCEDE SI NO HAY CIBERSEGURIDAD?

Si pensamos que la seguridad es estar libre de peligros o daños, uno de los factores más importantes de la formulación de políticas de ciberseguridad es la manera como se define qué constituye un daño en el ciberespacio. Sin las medidas de ciberseguridad adecuadas, aumenta la posibilidad de que surjan daños. Una interpretación amplia de lo que constituiría un daño cibernético incluiría:

Robo de datos con fines comerciales; por ejemplo, robo de números de tarjetas de crédito o robo de datos personales para su uso en *spam* o con fines de suplantación de identidad.

Acceso a datos para hacer espionaje industrial y adquirir ventajas competitivas.

Robo de datos con el fin de causar daño a la reputación, para desacreditar a un gobierno o a una entidad comercial, o para desacreditar a una persona o a un grupo de personas.

Acceso a los datos con el fin de recopilar inteligencia de un Estado extranjero o entidad no estatal.

Alteración o eliminación de datos con fines comerciales, políticos o económicos.

Pérdida de control sobre redes como resultado de ataques diseñados para debilitar o inhabilitar a un gobierno o entidad corporativa.

Manipulación del comportamiento de las personas, induciéndolas a descargar un programa malicioso (***malware***) o, inadvertidamente, a realizar otras acciones dañinas.

Amenazas al público como resultado de ataques diseñados para impedir el funcionamiento de los servicios públicos.

MEDIDAS DE CIBERSEGURIDAD

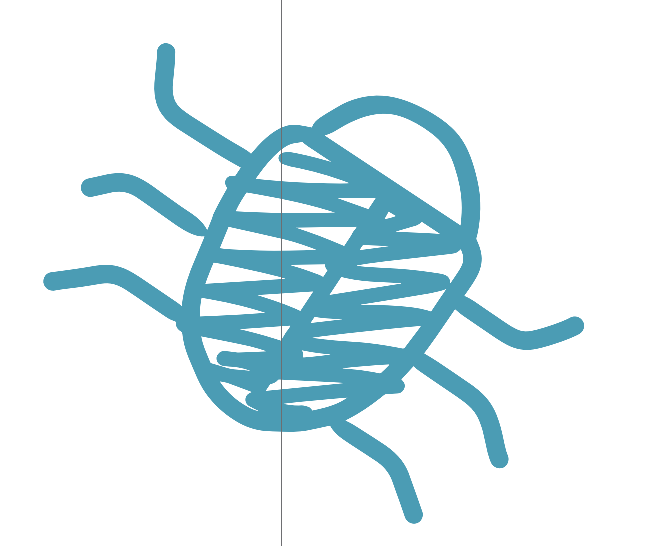
A pesar de la falta de acuerdo sobre los términos y los problemas que tratan, se toman medidas todo el tiempo para enfrentar los daños descritos anteriormente. Estos se pueden categorizar de la siguiente manera:

Medidas técnicas para mejorar la seguridad del *hardware* y *software* que constituyen los sistemas y redes informáticas. Estas pueden incluir pruebas de conformidad con normas técnicas como las criptográficas, la gestión de identidad y acceso, la gestión de riesgos de la cadena de suministro y la garantía del software.

Normatividad legal que desempeña un papel en la regulación de las condiciones bajo las que las entidades privadas y del sector público pueden adquirir, retener, procesar y compartir datos personales.

Algunas normas legales relevantes incluyen las leyes de protección de datos personales (consulte la páginas 48-50), las de intercambio de información como la Ley de Intercambio de Inteligencia de Ciberseguridad de los Estados Unidos (CISA, por su sigla en inglés[1]), así como las de ciberdelito.

Medidas procedimentales que incluyen procedimientos, directrices, decisiones institucionales y materiales educativos diseñados para minimizar el papel que desempeñan las personas (aparte de los computadores) en la creación o facilitación de inseguridades cibernéticas, por ejemplo, por medio de ataques de ingeniería social o el uso de contraseñas débiles.



DIMENSIONES DE LA POLÍTICA DE CIBERSEGURIDAD

Ya hemos explorado los orígenes del prefijo "ciber", el uso generalizado del término ciberseguridad, los daños relacionados con la ciberseguridad que contribuyen a la formulación de políticas públicas y las medidas adoptadas para contrarrestar esos daños. Ahora veremos cómo y dónde se formulan las políticas de ciberseguridad.

Para comenzar a responder estas preguntas, es necesaria cierta categorización. Con un tema tan complejo como la ciberseguridad, no hay una forma clara o definitiva de hacerlo. Si bien es inevitable un cierto traslape, estas tres categorías proporcionan una forma de entender la formulación de políticas de ciberseguridad hoy en día:

Seguridad de la información: la creación de normas y procesos técnicos y legales diseñados para proteger contra el acceso no autorizado a las redes de información y comunicaciones.

1 Nota del traductor: en adelante se omitirá esta aclaración.

Ciberdelito: medidas diseñadas para detectar, prevenir e investigar actividades ilegales. Esto incluye tanto los delitos en línea como aquellos fuera de internet que tengan un elemento en línea. Comprende, entre otras, la legislación sobre ciberdelitos, las medidas de vigilancia digital, las restricciones al contenido en línea y las iniciativas de intercambio de información.

Ciberconflicto: leyes y políticas que buscan gobernar, restringir o regular el uso de los **ciberataques**, operaciones, vandalismo y ciberrobo perpetrado por o contra actores estatales. Este aspecto de la política pública se relaciona con la creación de "cibernormas" o el esfuerzo por traducir el derecho internacional sobre conflictos bélicos entre Estados a un contexto en línea.

Ampliaremos cada una de estas áreas de políticas públicas en el Capítulo 2 (Seguridad de la información), el Capítulo 3 (Ciberdelito) y el Capítulo 4 (Ciberconflicto), y examinaremos las diversas medidas adoptadas en cada una, sus implicaciones para los derechos humanos y a que deberían prestar atención las personas defensoras de derechos humanos.

ACTORES DE LA CIBERSEGURIDAD Y SUS DESAFÍOS

ACTORES

Así como hay más de una forma de entender la ciberseguridad, hay más de un tipo de actor involucrado en la elaboración de políticas de ciberseguridad.

Si bien sería imposible enumerarlos a todos, en un plano muy general podemos identificar cinco categorías amplias de actores involucrados en la formulación de políticas de ciberseguridad: actores guberna-

mentales; instituciones intergubernamentales; comunidades técnicas y académicas; sector privado; y sociedad civil.

Cada tipo de actor enfrenta un conjunto diferente de desafíos en la era digital, lo que influye en su posicionamiento y participación en las políticas de ciberseguridad. Comprender los desafíos técnicos, legales y prácticos que enfrentan los responsables de las políticas de ciberseguridad y los actores interesados es un primer paso esencial para comprender cómo las personas defensoras de los derechos humanos pueden participar e influir en la formulación de políticas en este campo.

ACTORES GUBERNAMENTALES

Aunque podría decirse que todas las ramas gubernamentales deben ocuparse de la ciberseguridad de algún modo u otro, las organizaciones principalmente responsables de la ciberseguridad incluyen:

Organismos nacionales de normas técnicas, encargados de establecer y mantener estándares técnicos aplicables a la seguridad de la información. En los Estados Unidos, este organismo es el Instituto Nacional de Estándares y Tecnología (NIST).

Los equipos informáticos de respuesta a emergencias (**CERT**), también conocidos como equipos de preparación para emergencias informáticas y equipos de respuesta a incidentes de seguridad informática (**CSIRT**). Estos grupos de expertos, a menudo miembros de las agencias del orden público o de inteligencia, responden y buscan evitar incidentes de ciberseguridad, y con frecuencia también tienen la tarea de concienciar a la población.

Los ministerios de defensa, que están considerando cada vez más la posibilidad de un ciberconflicto y cómo responder a él.

Los ministerios del interior o de seguridad nacional, que generalmente supervisan las agencias del orden público y de inteligencia, coordinan la producción de estrategias nacionales de ciberseguridad y supervisan la ciberseguridad de la infraestructura crítica.

Los ministerios de asuntos exteriores o cancillerías, que coordinan la política exterior y las negociaciones sobre la política de ciberseguridad y derechos humanos.

Los ministerios de hacienda o de finanzas, que gestionan los presupuestos para la política de ciberseguridad.

Las agencias policiales, que responden no solo a los ciberdelitos (ej. robo de identidad, abuso o explotación sexual infantil en línea y venta de productos ilícitos), sino también a delitos fuera de internet con algún elemento en línea (ej. delitos planeados utilizando mensajes cifrados).

Las agencias de inteligencia, que generalmente tienen responsabilidades que abarcan la detección y prevención de incidentes de ciberseguridad y el mantenimiento de infraestructura crítica. Las agencias de inteligencia también son con frecuencia responsables de acciones que socavan la ciberseguridad, ya que algunas herramientas de vigilancia digital que utilizan (ej. ***malware***) explotan y manipulan las *vulnerabilidades* en sistemas y redes. Este es un buen ejemplo de cómo los gobiernos pueden tomar acciones contradictorias con respecto a la ciberseguridad.

Entidades gubernamentales que diseñan los planes o políticas gubernamentales. En Colombia, este organismo es el Departamento Nacional de Planeación (DNP).

DESAFÍOS QUE ENFRENTAN LOS ACTORES GUBERNAMENTALES

Dificultad de digitalizar los servicios gubernamentales para hacer que la prestación de servicios públicos sea más eficaz, y a la vez desarrollar capacidades y conocimientos técnicos de las agencias gubernamentales y el personal de la administración pública.

Falta de suficientes personas técnicas expertas en seguridad e ingeniería de seguridad para diseñar e implementar estrategias de ciberseguridad.

Riesgos que surgen de la naturaleza interjurisdiccional de la ciberseguridad, lo que implica que los países con débiles estrategias de ciberseguridad pueden socavar la ciberseguridad de todos los demás Estados.

Uso de herramientas de anonimización, como las criptomonedas, en delitos relacionados con internet, lo que dificulta la labor policial.
Constante aparición de nuevas tecnologías y sistemas que requieren sistemas de vigilancia actualizados.



Nuevos tipos de proveedores de servicios de comunicaciones que a menudo están domiciliados en otras jurisdicciones y requieren un tratamiento diferente al de las compañías de telecomunicaciones tradicionales.

Nuevas formas de ciberdelito, como el uso de ***ransomware***, robo de identidad, ***grooming*** y ciberacoso.

La necesidad de reaccionar frente a **ciberataques** y otras formas de conflicto interestatal a falta de normas internacionales acordadas que rijan el comportamiento de los Estados.

INSTITUCIONES INTERGUBERNAMENTALES

Debido a la naturaleza intrínsecamente interjurisdiccional de la ciberseguridad, el ciberdelito y el ciberconflicto, existe una gran variedad de instituciones intergubernamentales, foros y actores regionales e internacionales para las que la ciberseguridad es su tarea central o periférica.

Cuerpos de la ONU

El Grupo de Expertos Gubernamentales de las Naciones Unidas (GGE), un órgano convocado por el Primer Comité de Desarme y Seguridad Internacional de la Asamblea General de las Naciones Unidas para discutir y negociar normas internacionales de ciberseguridad.

Grupo de Trabajo de composición abierta sobre los avances en la esfera de las tecnologías de la información y las comunicaciones (TIC) en el contexto de la

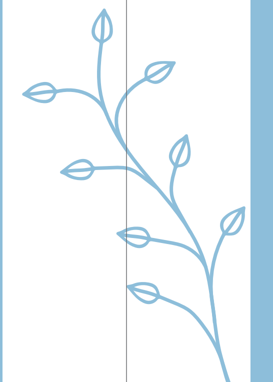
seguridad internacional (OEWG), también creado por el Primer Comité de Desarme y Seguridad Internacional de las Naciones Unidas en 2018. Su objetivo es estudiar normas internacionales existentes, identificar nuevas normas y estudiar la posibilidad de establecer un diálogo institucional regular. Se distingue del GGE en que participan todos los Estados miembros de la ONU interesados y en su naturaleza abierta, que significa que puede continuar operando hasta tanto los Estados miembros decidan disolverla.

El Comité contra el Terrorismo (CCT) del Consejo de Seguridad de la ONU, establecido después de los ataques terroristas de septiembre de 2001. Supervisa la implementación de la Resolución 1373 (2001), que requiere que los Estados detecten, criminalicen, enjuicien e investiguen actos terroristas y el financiamiento de terrorismo del terrorismo.

La Oficina de las Naciones Unidas contra la Droga y el Delito, que lleva a cabo estudios y construcción de capacidades en temas de ciberdelitos.

El Consejo de Derechos Humanos de la ONU y los órganos de tratados de la ONU (ej. el Comité de Derechos Humanos), que se ocupan principalmente de la ciberseguridad a través del lente de los derechos a la privacidad y la libertad de expresión.

La Unión Internacional de Telecomunicaciones (UIT), que tiene la responsabilidad general de las cuestiones técnicas y de ingeniería



relacionadas con la infraestructura de comunicaciones. En 2007, la UIT estableció un Grupo de Expertos de Alto Nivel sobre la ciberseguridad, que desarrolló una Agenda Global de Ciberseguridad para promover el desarrollo de soluciones y servicios para enfrentar las ciberamenazas. A través de este mecanismo, trabaja con los países en una serie de iniciativas de creación de capacidad de ciberseguridad.

Organismos internacionales

La Conferencia Global sobre el Ciberespacio (GCCS), concebida en 2011. Este organismo se reúne cada dos años con el objetivo de promover la cooperación práctica en temas del ciberespacio y debatir las normas que han de definir un comportamiento estatal responsable en el ciberespacio.

El Foro de Gobernanza de Internet (IGF) es un espacio de múltiples partes interesadas diseñado para reunir a gobiernos, empresas, academia, comunidad técnica y sociedades civiles alrededor de la misma mesa para debatir temas de gobernanza de internet.

Organismos regionales

El Consejo de Europa, compuesto por 47 Estados miembros, coordina a las 68 partes firmantes del Convenio de Budapest sobre el ciberdelito (consulte la página 65-67), 65 de las que han ratificado este instrumento. Este es el primer tratado internacional que aborda el ciberdelito mediante la armonización de las leyes nacionales y el fortalecimiento de la cooperación interestatal.

La Cooperación Económica Asia-Pacífico (APEC), la Unión Africana (UA), la Asociación de Naciones del Asia Sudoriental (ASEAN), la Organización de Estados Americanos (OEA) y la Organización para la Seguridad y la Cooperación en Europa (OSCE) tienen grupos de trabajo y comités dedicados a la ciberseguridad y el ciberdelito. Por ejemplo, la OEA tiene un Grupo de trabajo sobre ciberdelitos, además de que el Comité Interamericano contra el Terrorismo (CICTE) también se ocupa de cuestiones de ciberseguridad.

La Unión Europea (UE) tiene una estrategia de ciberseguridad desde 2013, diseñada para promover la construcción de capacidades de los Estados miembros, la cooperación y el intercambio de información. Además, sus órganos trabajan en cada uno de los diferentes aspectos de la ciberseguridad. Estos incluyen la Comisión Europea, el Parlamento Europeo, el Consejo de Europa, el EU-CERT y el Servicio Europeo de Acción Exterior.

¿QUIERE SABER MÁS SOBRE EL ROL DE LA ORGANIZACION DE ESTADOS AMERICANOS EN CIBERSEGURIDAD?

HAGA CLIC



PARA LEER DERECHOS HUMANOS Y SEGURIDAD DIGITAL: UNA PAREJA PERFECTA.



DESAFÍOS DE LOS ORGANISMOS INTERGUBERNAMENTALES

Desigualdad en los niveles de desarrollo, infraestructura técnica y acceso a internet entre Estados y regiones.

Opiniones divergentes entre los Estados en cuanto a las virtudes del enfoque de múltiples partes interesadas (*multistakeholder*), las estrategias de gobernanza de internet, y el control y restricción de contenidos.

Lentitud de los procesos multilaterales en comparación con los avances tecnológicos.

Falta de confianza entre los Estados y dificultad de abordar temas de seguridad en los organismos intergubernamentales, lo que aumenta la necesidad de encontrar soluciones bilaterales, en lugar de multilaterales.

Diferentes niveles de prioridad otorgados a la ciberseguridad en diversos Estados, con diferentes responsabilidades asignadas a distintos organismos y ministerios en cada país.

COMUNIDADES TÉCNICA Y ACADÉMICA

Existen más de 200 organizaciones de estandarización (SDO) que definen normas técnicas relevantes para la ciberseguridad. Algunas de los más destacadas son:

La Organización Internacional de Estandarización (ISO), que reúne a nivel internacional a los organismos nacionales de normas técnicas.

El Grupo de Trabajo de Ingeniería de Internet (IETF), una organización de estandarización abierta, sin requisitos formales de membresía que define y promueve normas voluntarias de internet, particularmente aquellas que conforman particularmente aquellas que conforman su conjunto de protocolos. Cualquier persona puede participar en el IETF y las decisiones se toman por consenso. Existe un grupo de trabajo creado para tratar específicamente con la seguridad, así como un grupo de investigación que estudia las implicaciones para los derechos humanos en la capa técnica (consulte la página 112).

El Internet Architecture Board (IAB) supervisa al IETF y es el comité encargado de vigilar el desarrollo técnico y de ingeniería de internet. Originalmente era un organismo del Gobierno de los Estados Unidos, pero pasó a ser independiente en 1992. Además de supervisar los protocolos y procedimientos de la red, el IAB trabaja con la autoridad de números asignados de internet.

La Corporación de Internet para Nombres y Números Asignados (ICANN) es una organización sin fines de lucro responsable de coordinar el mantenimiento de varias bases de datos de identificadores únicos relacionados con los espacios de nombres de internet. Su actividad más visible es administrar el sistema de nombres de dominio (DNS), los dominios de nivel superior, el funcionamiento de los servidores de raíz y la asignación de espacios de direcciones de protocolo de internet para IPv4 e IPv6.

DESAFÍOS DE LAS COMUNIDADES TÉCNICA Y ACADÉMICA

Aseguramiento de que los estándares técnicos voluntarios acordados se adopten e implementen ampliamente.

Esfuerzos abiertos y encubiertos por parte de los Estados para socavar las normas técnicas o controlar el proceso de elaboración de normas técnicas.

Falta de capacidad de estas comunidades o inexistencia de organizaciones para atender estos temas en algunos países, sobre todo, del Sur global.

ACTORES DEL SECTOR PRIVADO

Las instituciones financieras son algunos de los principales creadores y promotores de normas técnicas relacionadas con la ciberseguridad, lo que no resulta sorprendente dado que se encuentran entre las entidades más seriamente afectadas por los **ciberataques**.

Los fabricantes de software y hardware tienen la obligación de garantizar la seguridad de sus productos y en toda la cadena de suministro.

Las empresas de tecnología y los proveedores de servicios y aplicaciones de internet a menudo se oponen a las medidas que los Estados toman en nombre de la ciberseguridad o están en conflicto con los gobiernos sobre la responsabilidad civil y/o penal del ciberdelito. Cada vez se

les reconoce más como actores clave en las iniciativas de ciberdelitos y en el ámbito de la política de ciberseguridad.

Los proveedores de productos y servicios de antivirus y ciberseguridad son fundamentales para ayudar a los actores públicos y privados a defenderse y responder a las ciberamenazas. También son una fuente de investigación y datos sobre la ciberseguridad, por ejemplo, con respecto a la frecuencia y los tipos de violaciones a la ciberseguridad.

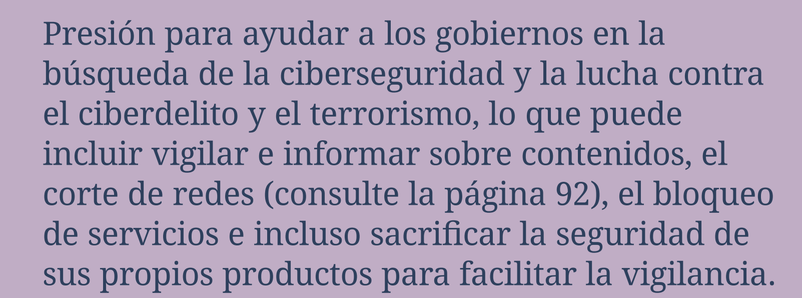
Los proveedores de telecomunicaciones mantienen la infraestructura y proporcionan acceso a internet. En muchos países, los proveedores de telecomunicaciones son o eran de propiedad estatal, y como resultado, sus intereses a menudo están alineados con los intereses estatales en este sector.

Las empresas de tecnología de vigilancia venden productos de vigilancia y herramientas de ***hacking*** en el mercado privado a los gobiernos.

DESAFÍOS DEL SECTOR PRIVADO

Dificultades para operar en distintas jurisdicciones con leyes, sanciones y regímenes regulatorios dispares.

Posible daño grave a la reputación y posible responsabilidad civil al ser víctima o responsable de un incidente de ciberseguridad.

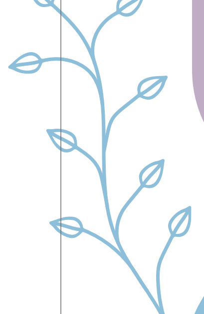


Presión para ayudar a los gobiernos en la búsqueda de la ciberseguridad y la lucha contra el ciberdelito y el terrorismo, lo que puede incluir vigilar e informar sobre contenidos, el corte de redes (consulte la página 92), el bloqueo de servicios e incluso sacrificar la seguridad de sus propios productos para facilitar la vigilancia.

Necesidad de construir capacidad interna en seguridad de la información y redes.

Incentivos para no divulgar datos sobre riesgos y **ciberataques** para evitar preocupación por la privacidad de los datos y potencial daño a la reputación.

Equilibrio entre un modelo de negocio rentable y una seguridad robusta para la persona usuaria y la empresa.



SOCIEDAD CIVIL

Podría decirse que el jugador menos activo en el ámbito de la política de ciberseguridad es la sociedad civil. Si bien las personas defensoras de derechos humanos hacen un trabajo importante en varias áreas sobre políticas de ciberseguridad, aún existen otras en las que la sociedad civil no participa sustancialmente. Los factores que contribuyen a esto pueden incluir:

La falta de fondos y de capacidad para seguir los debates sobre políticas de ciberseguridad;

la naturaleza cerrada de muchos foros de políticas de ciberseguridad; y

la falta de capacidad técnica.





La sociedad civil está especialmente comprometida con algunos temas de política que se superponen con la ciberseguridad, incluida la gobernanza de internet, los debates sobre privacidad y vigilancia, y la intersección entre los temas de internet y la libertad de expresión, entre otros. Otros grupos trabajan en temas como la protección de la niñez, que están estrechamente relacionados con la dimensión del cibercrimen (véase el Capítulo 3).

DESAFIÓS DE LA SOCIEDAD CIVIL

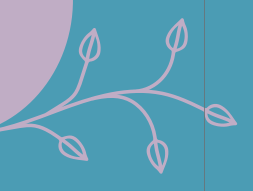
Proliferación de actividades gubernamentales y corporativas bajo el rubro de la ciberseguridad, con poca claridad sobre lo que se está haciendo y con qué fin.

Poca claridad de leyes y políticas relacionadas con internet así como la falta de transparencia en torno a las agencias gubernamentales que monitorean y controlan el uso de internet.

Falta de transparencia en el uso por parte de los gobiernos de cibercapacidades ofensivas.

Cambio vertiginoso y constante de las tecnologías, falta de comprensión del público y alfabetización digital (incluidos los bajos niveles de uso y comprensión de las herramientas para mejorar la privacidad por parte del público en general) y dificultad de hacer que los problemas técnicos sean accesibles a un público amplio.

Falta de espacios efectivos de participación.



¿CÓMO SE RELACIONAN LOS DERECHOS HUMANOS CON LA CIBERSEGURIDAD?

A menudo se dice que la ciberseguridad se refiere a la protección de la información y de las redes. Ambos son importantes desde una perspectiva de derechos humanos, pero ¿por qué?

INFORMACIÓN

La información es fundamental para el funcionamiento de nuestra vida cotidiana. Las personas generan y comparten enormes cantidades de datos personales todos los días, desde correos electrónicos y datos de salud hasta datos bancarios e historiales laborales. Estos datos, particularmente cuando se reúnen, pueden revelar fácilmente detalles muy sensibles sobre una persona, por ejemplo, su orientación sexual, actividad política o ubicación geográfica.

Estos datos generalmente pertenecen a entidades del sector privado o público, quienes los gestionan y almacenan. Desde el punto de vista de los derechos humanos, esto tiene serias implicaciones. Sin las medidas de ciberseguridad adecuadas, no solo es posible acceder y robar la información, sino que se puede eliminar, alterar y modificar.

El ***hackeo*** a la Oficina de Gestión de Personal de los Estados Unidos en 2015, por ejemplo, expuso la información personal confidencial de 22 millones de personas, incluido su historial de salud mental y detalles sobre el abuso de drogas y alcohol. Este tipo de ataques tiene un impacto directo en los derechos humanos, incluido el derecho a la privacidad, y puede afectar directamente las vidas de las personas más allá de sus interacciones en línea. Sin embargo, el Gobierno de los Estados Unidos presentó el ***hackeo*** como un incidente puramente diplomático, y prometió una rápida retaliación contra el gobierno extranjero considerado responsable, en lugar de reflexionar sobre si dicha cantidad de datos deberían haberse recopilado y almacenado, dadas las débiles salvaguardas establecidas (consulte la página 80 para obtener más ejemplos de violaciones de datos personales).

Además de los datos personales en manos de entidades del sector privado o público, existen datos estatales y corporativos.

Los datos estatales también pueden ser confidenciales, incluso si no se relacionan con una persona a la manera que lo hace los datos personales. Pueden incluir información sobre negociaciones comerciales, inteligencia extranjera, ubicación de tropas, secretos militares y procesos judiciales.

Los datos corporativos pueden incluir información sobre acuerdos, activos, patentes y secretos comerciales.

OPERACIÓN *BUCKSHOT YANKEE*

En 2008, redes militares dirigidas por el Comando Central de los Estados Unidos fueron atacadas por un gusano que originalmente entró en el sistema a través de una memoria USB infectada que contenía código malicioso o *malware*. El *malware* se instaló automáticamente en el sistema y lo escaneo en búsqueda de datos, incluyendo planes operativos de alto secreto, que luego podía enviar a un controlador remoto. Tomó 14 meses limpiar el sistema. El incidente motivó la creación del Comando Cibernético de los Estados Unidos.

REDES

Las redes son la infraestructura que transmiten y almacenan información y facilita la conectividad de los dispositivos.

Desde el punto de vista de los derechos humanos, las redes son signifiativas porque el funcionamiento de cada servicio público y privado importante depende de su seguridad. Esto incluye los servicios de telefonía celular, pagos electrónicos, sistemas bancarios, redes de transporte público, suministro de gas y electricidad, hasta el funcionamiento de los semáforos. Los esfuerzos para socavar el funcionamiento de estas redes pueden tener efectos inmediatos y directos en la vida de las personas, especialmente a medida que más personas y objetos están conectados a internet.

Desde esta perspectiva, las medidas diseñadas para proteger la información y las redes pueden considerarse como un requisito previo para el disfrute de un gran número de derechos humanos:

- el derecho a la intimidad y a la protección de la información personal;
- el derecho a la libertad de expresión y el acceso a la información;
- el derecho a la libertad de asociación y reunión;
- el derecho a la libertad y seguridad de la persona; y
- los derechos de las niñas, niños y adolescentes a estar libres de explotación y abuso.

LAS LUCES SE APAGAN EN UCRANIA

En diciembre de 2015, la compañía eléctrica ucraniana Prykarpattyaoblenergo informó de un apagón en la capital regional Ivano-Frankivsk. Otras dos empresas de servicios públicos experimentaron apagones al mismo tiempo, pero no los reportaron. El mismo *malware*, BlackEnergy, fue identificado en los tres apagones, lo que permite sugerir que fueron resultado de un ciberataque. El análisis del *malware* reveló que estaba diseñado para borrar la memoria del sistema. El Gobierno ucraniano acusó a Rusia de perpetrar el ataque.





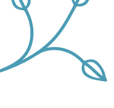
MEDIDAS DE CIBERSEGURIDAD, ¿UNA FORMA DE OCULTAR VIOLACIONES DE DERECHOS HUMANOS?

La formulación de políticas de ciberseguridad también puede tener graves consecuencias en el disfrute de los derechos humanos. Como hemos mostrado anteriormente, las medidas de política se toman con el objetivo explícito de prevenir, detectar o investigar amenazas y delitos en línea. Sin embargo, estas medidas también pueden limitar el disfrute de los derechos humanos por parte de la ciudadanía. Algunos ejemplos incluyen:

medidas para evitar el **anonimato** o la confidencialidad en línea, incluida la restricción de servicios cifrados. Estos a menudo se explican como una forma para combatir el ciberdelito, pero pueden paralizar la libre expresión y menoscabar seriamente la capacidad de las personas de ejercer su derecho a la intimidad. Sin acceso a servicios cifrados, las personas defensoras de derechos humanos, periodistas, minorías y grupos de oposición no pueden asociarse libremente sin temor a que les detecten (consulte la página 82);

medidas punitivas y restricciones contra grupos **hacktivistas** en nombre de la ciberseguridad, que a menudo son desproporcionadas e impiden el derecho a la libre expresión, a la información y a la asociación;

la imposición de sistemas de **vigilancia masiva**, y la retención y localización obligatoria de datos, que socava la esencia del derecho a la intimidad y crea sociedades vigiladas, privadas de pensamiento progresivo, innovación y creatividad (consulte página 74);



el bloqueo de contenido, la imposición de filtros de internet y la criminalización del uso de sistemas informáticos para difundir contenido restringido, que impide el libre funcionamiento de internet y constituye una censura en nombre del trabajo policial;

la manipulación de la infraestructura, los cortes de internet y la reducción de su velocidad durante eventos políticos, elecciones y manifestaciones, que ponen en peligro los derechos de las personas usuarias a la expresión y a la protesta (consulte la página 92); o

el almacenamiento de **vulnerabilidades de día cero** para su uso en ciberoperaciones ofensivas, que en realidad socava los objetivos de ciberseguridad al hacer que la información y las redes sean menos seguras y más propensas a los ataques (consulte la página 85).

Cuatro ejemplos recientes ilustran la aplicación generalizada de la ciberseguridad en la formulación de políticas públicas:



En 2014, el Gobierno de Paraguay propuso un fallido proyecto de ley que ordenaba a los proveedores de servicios de internet, incluidos los operadores de telefonía móvil, a almacenar **metadatos** de todas las comunicaciones de internet durante 12 meses. Estas bases de datos serían accesibles a las autoridades con “fines de investigación criminal”.



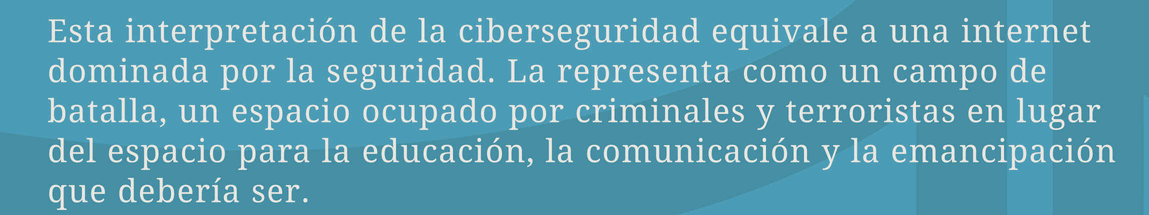
En 2015, China publicó un proyecto de ley de ciberseguridad que exige a los proveedores de servicios que conserven los datos personales de las personas usuarias y de las claves de **cifrado** al interior de China.



Israel asignó USD 26 millones en fondos de ciberseguridad a iniciativas digitales destinadas

a combatir los intentos de “deslegitimar” a Israel, en particular la Campaña de Boicot, Desinversión y Sanciones (BDS).

4 En 2015, Australia aprobó una controversial enmienda a su Ley de Telecomunicaciones (interceptación y acceso) para introducir la obligación legal a los proveedores de servicios de telecomunicaciones de conservar, durante dos años, los **metadatos** de las telecomunicaciones. Las autoridades del orden público argumentaron que los datos de telecomunicaciones son fundamentales para las investigaciones penales y que solo a través de la legislación pueden estar seguros de que estarán.

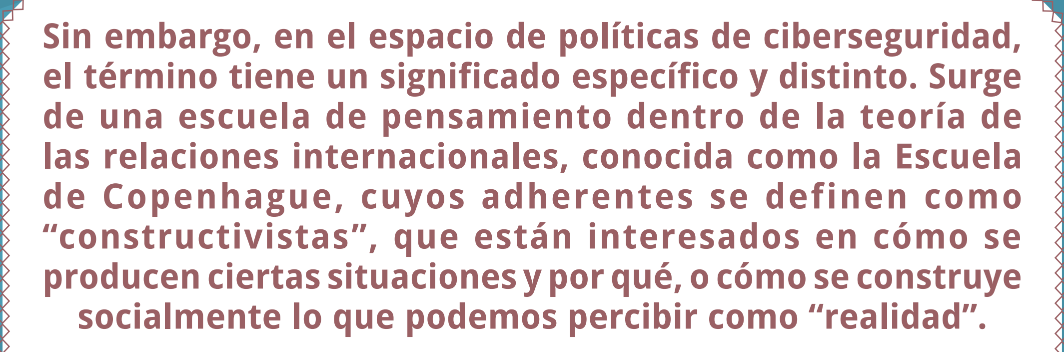


Esta interpretación de la ciberseguridad equivale a una internet dominada por la seguridad. La representa como un campo de batalla, un espacio ocupado por criminales y terroristas en lugar del espacio para la educación, la comunicación y la emancipación que debería ser.

Los efectos adversos de las políticas de ciberseguridad sobre los derechos humanos pueden no ser siempre intencionales, aunque pueden ser previsibles y evitables siempre que los gobiernos inviertan el tiempo, los recursos y la voluntad para comprometerse con los derechos humanos. Por esta razón en particular, es fundamental que las personas defensoras de derechos humanos participen en la toma de decisiones de ciberseguridad.

SECURITIZACIÓN

Una búsqueda en línea del concepto “securitización” dará como resultado una serie de definiciones, la mayoría de ellas relacionadas con el campo de la finanzas.



Sin embargo, en el espacio de políticas de ciberseguridad, el término tiene un significado específico y distinto. Surge de una escuela de pensamiento dentro de la teoría de las relaciones internacionales, conocida como la Escuela de Copenhague, cuyos adherentes se definen como “constructivistas”, que están interesados en cómo se producen ciertas situaciones y por qué, o cómo se construye socialmente lo que podemos percibir como “realidad”.

Según la Escuela de Copenhague, la securitización es el proceso por el que ciertos actores (conocidos como actores securitizadores) transforman un asunto en uno de “seguridad”. Este asunto, una vez enmarcado de esta forma, puede atraer desproporcionadamente una parte de la atención y de los recursos a la amenaza que representa, y justificar medidas de seguridad extraordinarias –por ejemplo, un estado de emergencia o un apagón de internet–. Esta teoría se utiliza a menudo para explicar por qué algunas amenazas a la vida humana –por ejemplo, el terrorismo– reciben más atención que otras en los medios de comunicación y en la formulación de políticas.

La Escuela identifica las siguientes características claves de las amenazas que están “securitizadas”:

* **están enmarcadas no solo como dañinas, sino también como nefastas, inminentes y existenciales (es decir, como una amenaza para la existencia o supervivencia humana),**
* **se enmarcan como una amenaza a la soberanía nacional y a la autonomía política, y se hace hincapié en la protección de la supervivencia y los valores colectivos por**
* **encima de la protección de las personas.**

Hay muchos “actores de securitización” potenciales involucrados en el proceso, que pueden incluir al funcionariado público, otras personas responsables de la formulación de políticas, personalidades corporativas o grupos de presión, y medios de comunicación.



¿CÓMO SERÍA UN CIBERESPACIO BASADO EN LOS DERECHOS HUMANOS?

En junio de 2012, el Consejo de Derechos Humanos de las Naciones Unidas declaró en una resolución que “[l]os mismos derechos que la gente tiene fuera de internet, deben ser protegidos dentro de ella”. Sin embargo, desde este momento histórico, la ONU, sus diversos organismos y otros mecanismos regionales de derechos humanos se han tardado en proporcionar más orientación sobre lo que requieren los Estados para garantizar lo anterior.

Esta es un área en evolución de los derechos humanos, y hay pocas respuestas definitivas sobre lo que los gobiernos y los actores privados deben y no deben hacer cuando se trata del ciberespacio. Sin embargo, hay una serie de instrumentos internacionales y regionales que ofrecen alguna orientación sobre el tema. Ellos ordenan que cualquier medida, incluyendo aquella adoptada en nombre de la ciberseguridad y que resulte en la restricción de los derechos humanos en la era digital, debe cumplir con los siguientes estándares:

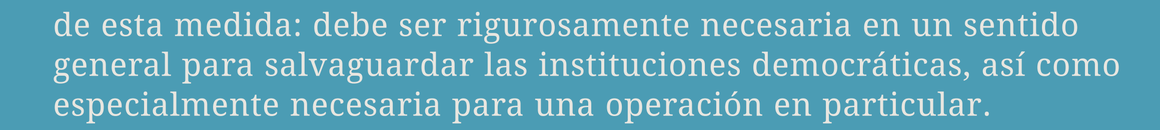
ESTAR PRESCRITA POR LA LEY

No es suficiente que la medida que prohíba actividades en internet o el uso de ciertos servicios sea parte de políticas o acuerdos con proveedores de servicios. Debe estar prevista por una legislación que sea clara, pública y transparente. Además, su aplicación debe ser supervisada por un órgano judicial o independiente. En el caso de vigilancia secreta, debido al alto riesgo de una implementación arbitraria de una medida de vigilancia, se requiere autorización judicial.



SER NECESARIA EN UNA SOCIEDAD DEMOCRÁTICA

Necesario significa más que “útil” o “deseable”. Puede que resulte útil prohibir el uso del **cifrado** de extremo a extremo, pero eso no hace que sea necesario para alcanzar los objetivos de ciberseguridad. En el caso de la vigilancia secreta, se debe demostrar la “estricta necesidad”

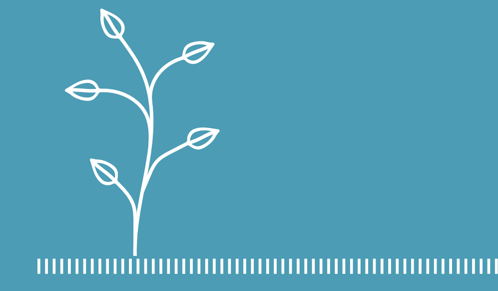


de esta medida: debe ser rigurosamente necesaria en un sentido general para salvaguardar las instituciones democráticas, así como especialmente necesaria para una operación en particular.

SER UNA RESPUESTA PROPORCIONAL A ESOS OBJETIVOS

El daño causado por una restricción propuesta no debe superar el beneficio obtenido. Al considerar el daño causado en el contexto de una restricción que se aplique a internet es fundamental recordar el papel central que desempeñan los derechos a la libertad de expresión, asociación y reunión para garantizar una democracia funcional y responsable. Además, hay que considerar que una restricción que se aplique a internet puede tener una aplicación increíblemente amplia, que a su vez puede afectar a personas de todas partes del mundo. Cuando una restricción tiene un impacto generalizado en las personas que no representa una amenaza para la ciberseguridad, la carga de responsabilidad de justificar la restricción recae en el Estado.

Donde haya medidas menos intrusivas que logren el mismo objetivo, debe optarse por estas. Además, debe proporcionarse una justificación pública basada en evidencia para imponer cualquier restricción. Las medidas específicas son preferibles a las medidas generales. Un análisis de proporcionalidad debe tener en cuenta la fuerte posibilidad de que, por ejemplo, una medida que restrinja el **cifrado** y el **anonimato** será explotada por las mismas redes criminales y terroristas que la limitación pretende evitar.





LA CIBERSEGURIDAD COMO SEGURIDAD DE LA INFORMACIÓN

¿Quién sabe qué sobre mí?

La seguridad de la información consiste en garantizar que los datos creados, recopilados, generados, procesados o almacenados por entidades privadas y públicas estén protegidos contra el acceso no autorizado, la manipulación, el robo y la explotación.

En este sentido, la ciberseguridad consiste en aplicar medidas para hacer que la información y las redes sean más seguras.

¿Cómo se vuelve más segura la información? Eso depende en gran parte de las amenazas y actores de quienes se está tratando de protegerla y de las medidas (técnicas, legales o procedimentales) que se utilicen para hacerlo.

UNA COMPRENSIÓN DIFERENTE DE LA SEGURIDAD DE LA INFORMACIÓN

Como explicamos en el Capítulo 1 (consulte la página 13), la falta de definiciones acordadas significa que los diferentes actores se apropian de los términos para distintos fines y el término "seguridad de la información" no es una excepción. China y Rusia han propuesto previamente un Código Internacional de Conducta para la Seguridad de la Información que insta a la cooperación internacional a frenar "la difusión de información que incite al terrorismo, al secesionismo o al extremismo o que socave la estabilidad política, económica y social de otros países, así como su entorno espiritual y cultural".

Cada agencia gubernamental, empresa u otra entidad encontrará diferentes formas de riesgo para la ciberseguridad dependiendo de qué información contienen y procesan, con qué propósito y de qué manera. Por ejemplo, un fondo de cobertura podría percibir que el mayor riesgo para su ciberseguridad es el robo de información confidencial sobre operaciones bursátiles y la manipulación de mercados financieros, mientras que la divulgación de la información personal de su personal podría considerarse un riesgo menor.

Cada agencia gubernamental, empresa u otra entidad encontrará diferentes formas de riesgo para la ciberseguridad

Una autoridad fiscal consideraría que el acceso a los datos personales e información tributaria es su mayor riesgo. De hecho, dos **ciberataques** al Servicio de Impuestos Internos (IRS) de los Estados Unidos en 2015 y 2016 resultaron en la adquisición por parte de "ladrones de identidad" de más de 100,000 códigos PIN utilizados para acceder a los archivos de impuestos.



La innovación tecnológica durante los próximos años tendrá un impacto aún más significativo en nuestra forma de vida. Esta innovación es fundamental para nuestra prosperidad económica, pero traerá nuevas vulnerabilidades de seguridad. La internet de las cosas conectará decenas de miles de millones de nuevos dispositivos físicos que podrían ser explotados. [...] Los ciberdelincuentes siguen siendo la ciberamenaza más generalizada para el sector financiero de los Estados Unidos. Utilizan el ciberespacio para realizar robos, extorsiones y otras actividades delictivas.

Testimonio del entonces Director de Inteligencia Nacional, James Clapper, ante el Comité de Servicios Armados del Senado de los Estados Unidos el 9 de febrero de 2016.

En una evaluación de amenazas ante el Comité de Servicios Armados del Senado de los Estados Unidos el 9 de febrero de 2016, el entonces Director de Inteligencia Nacional, James Clapper, habló de los riesgos que plantean los sistemas y redes de información desprotegidos. Gobiernos y empresas de todo el mundo coinciden en la opinión de que la ciberseguridad, vista como seguridad de la información, es una prioridad política clara y preeminente. Sin embargo, acalorados debates continúan sobre la mejor manera de lograr este objetivo.

NORMAS TÉCNICAS INTERNACIONALES

Hay más de 1,000 publicaciones que pretenden establecer normas técnicas sobre la ciberseguridad, pero ninguna abarca su totalidad. Esto ha resultado en el desarrollo intermitente y desigual de normas técnicas. Un informe del Instituto Nacional de Normas y Tecnología (NIST) de los Estados Unidos de diciembre de 2015, que identifica diez áreas principales para la estandarización de la ciberseguridad (incluidas, por ejemplo, técnicas criptográficas), señala que en apli-

caciones clave como la computación en la nube, la gestión de emergencias o votación, por lo general, solo hay unas pocas normas técnicas disponibles; mientras que en muchas áreas no existen aún o están en desarrollo. Las normas técnicas existen solo en algunas áreas selectas de la estandarización, como la seguridad de la red para aplicaciones de votación.

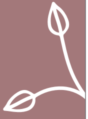
NORMA ISO 9564 – GESTIÓN DEL NÚMERO DE IDENTIFICACIÓN PERSONAL (PIN)

Un ejemplo de un estándar técnico es la ISO 9564, que se refiere a la gestión del PIN y la seguridad en la banca minorista.

El mantenimiento de la seguridad en los sistemas bancarios modernos se basa en la interoperabilidad entre los bancos, los comercios y los emisores de tarjetas, lo que requiere un conjunto común de normas y prácticas en cuanto a la forma en que se adquieren, autentican y transmiten los números de identificación personal (PIN).

Este estándar ISO proporciona esas reglas y prácticas: desde la longitud de los PIN y la especificación de los dispositivos de entrada de PIN, hasta la emisión y cifrado de PIN.

Tradicionalmente, el desarrollo de normas técnicas ha sido impulsado por el mercado y suele ser reactivo en lugar de anticiparse a las necesidades futuras. Estas normas son formuladas por organizaciones de estandarización (SDO) en todo el mundo, principalmente organizaciones voluntarias compuestas por individuos, personas expertas y representantes de la industria, que trabajan por consenso. De esta manera, el desarrollo de normas técnicas es, a menudo, un proceso “de abajo hacia arriba”. Sin embargo, en algunos países los organismos nacionales de estandarización están muy influenciados por el Gobierno. Existe una marcada diferencia entre el enfoque de los Estados Unidos, que depende en gran medida del sector privado para impulsar el desarrollo de estándares, y la Unión Europea, que adopta un enfoque más vertical (por ejemplo, a través del Instituto Europeo de Normas de Telecomunicaciones).



Hay más de 1,000 publicaciones que pretenden establecer normas técnicas sobre la ciberseguridad, pero ninguna abarca su totalidad.

Existe bastante consenso sobre el papel esencial que desempeñan las SDO en el desarrollo de normas para la ciberseguridad y sobre cuál debería ser el objetivo de este desarrollo. Sin embargo, el proceso de negociación en el desarrollo de normas para la ciberseguridad puede ser lento, opaco y cerrado a la participación de personas externas. El entorno, según el NIST, está cada vez más politizado, ya que los países han empezado a “promover” intereses políticos específicos en torno a diferentes SDO, considerando el proceso de desarrollo de normas como una buena oportunidad para promover la adopción de políticas que reflejen agendas particulares.

Además de la falta de normas coherentes, las entidades del sector privado también se quejan de la falta de información y orientación en relación con la implementación de las normas, y de la falta de claridad sobre qué normas cumplir para adaptarse mejor a sus necesidades y demográfica organizacional. Además, puede ser difícil para ellas saber qué normas o guías se deben tomar como “mejores prácticas”. **Las empresas del sector privado están abrumadas con la cantidad de normas en ciertas áreas y su notable ausencia en otras**, como aquellas relacionadas con la forma en las que su personal y contratistas deben actuar para proteger la ciberseguridad.

De hecho, existe un énfasis excesivo en las normas técnicas, excluyendo aquellas relacionadas con los procesos (consulte la página 17). Un estudio de 2015 que encargó el Gobierno del Reino Unido reveló que existen más de 1,000 publicaciones sobre la ciberseguridad en todo el mundo, el 67 por ciento de las cuales se centran en los estándares de ciberseguridad de las organizaciones, y solo el 3 por ciento en los de las personas.

OBLIGACIONES Y RESPONSABILIDADES LEGALES

El panorama jurídico de la ciberseguridad está marcado por las ausencias. No se ha acordado un marco jurídico global para la protección de datos. No hay un intercambio de información coherente entre entidades públicas y privadas para alcanzar los fines de ciberseguridad, al igual que los objetivos de orden público y seguridad nacional. Para las organizaciones globales que operan en una variedad de mercados, estos factores impiden cada vez más la adopción e implementación de estrategias de ciberseguridad.

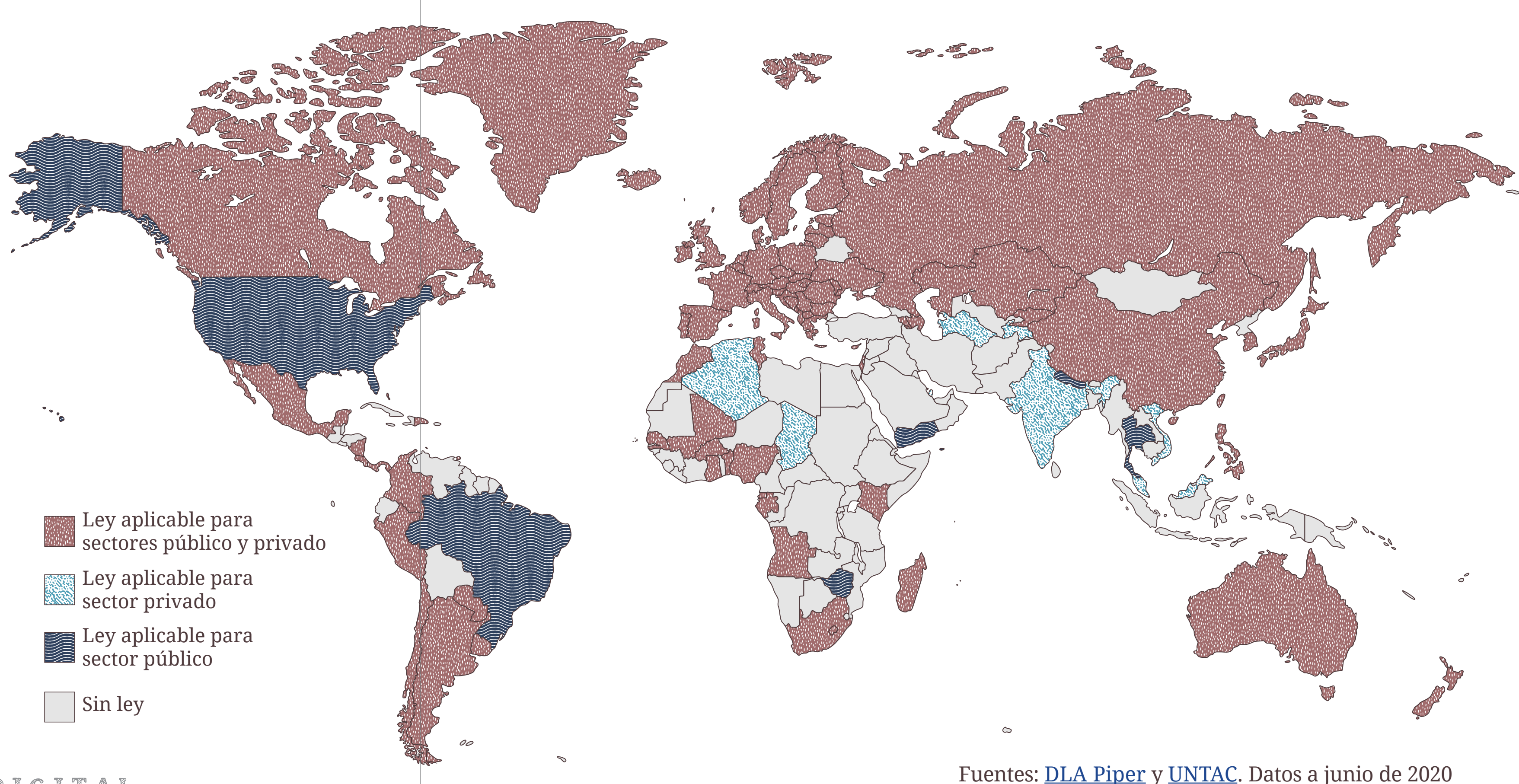
La ausencia de un acuerdo global y, en particular, transatlántico, sobre normas de protección de datos saltó a la luz pública con la decisión del Tribunal de Justicia de la Unión Europea en el caso *Schrems* v. *Comisionado de Protección de Datos sobre el Acuerdo "Safe Harbour"* en 2015. El caso invalidó la base jurídica sobre la cual las empresas podrían transferir los datos recopilados en la Unión Europea hacia los Estados Unidos para su procesamiento. El fundamento del fallo recayó en las dudas sobre la disparidad entre la protección de datos de la Unión Europea y los Estados Unidos, pero el mismo tiene ramificaciones globales. A medida que las empresas en Europa buscan externalizar tareas de sus procesos de negocios a países fuera de las fronteras europeas, los regímenes de privacidad y protección de datos en Asia, América Latina y África estandarizarán cada vez más sus marcos regulatorios con Europa.

Tras la sentencia del Tribunal de Justicia, la Unión Europea y los Estados Unidos adoptaron un nuevo acuerdo, conocido como el "Escudo de Privacidad", que no ha estado exento de críticas y riesgos de ser suspendido por ambas partes. Sin embargo, puede ser necesaria una solución a largo plazo para reducir la disparidad entre los enfoques de protección de datos. Desde hace mucho tiempo, Europa ha adoptado un enfoque regulatorio activo para la protección de datos personales, mientras que los Estados Unidos ha preferido los regímenes de regulación propia y sectorial. Esto crea numerosos problemas de cumplimiento para las empresas que operan en ambas jurisdicciones.

A medida que crece el número de empresas que operan en varias jurisdicciones, y otros países del mundo adoptan una legislación que imita el enfoque de la Unión Europea, el argumento comercial para llegar a un acuerdo global sobre protección de datos solo se hace más fuerte.

La Unión Europea y los Estados Unidos celebraron un acuerdo general (*umbrella agreement*) sobre protección de datos en septiembre de 2015, diseñado para aplicarse a la transferencia transatlántica de datos entre agencias gubernamentales (en lugar de entre empresas), lo que puede considerarse como un paso de normalización de los dos regímenes, aunque no definitivo.

LEYES DE PROTECCIÓN DE DATOS EN EL MUNDO



Fuentes: DLA Piper y UNTAC. Datos a junio de 2020

PRÁCTICAS DE INTERCAMBIO DE INFORMACIÓN

En 2015, tanto los Estados Unidos como Europa adoptaron leyes relacionadas con la divulgación de información por parte de entidades corporativas y entre agencias gubernamentales con fines de ciberseguridad. La Ley de Intercambio de Información sobre Ciberseguridad (CISA) de los Estados Unidos, promulgada en diciembre de 2015, permite a las empresas de internet y a otras entidades del sector privado estadounidense compartir información sobre el tráfico de internet con el gobierno de dicho país, especialmente en el caso de amenazas de ciberseguridad. La ley recibió fuertes críticas por parte de personas defensoras de derechos humanos y organizaciones de la sociedad civil, preocupadas por que otorgaba una inmunidad general ante sanciones civiles y penales a empresas que compartieran información personal sin una orden judicial. La ley permite que se compartan datos con una amplia gama de agencias gubernamentales, desde el FBI y la NSA hasta la agencia federal de impuestos. En un entorno ya marcado por las preocupaciones sobre la transparencia y la rendición de cuentas por parte de las agencias estadounidenses de inteligencia, muchos grupos temen que CISA funcione como otra forma de vigilancia de la ciudadanía. Sin embargo, el Gobierno sostiene que es necesario alentar a las empresas a compartir datos que son esenciales para detectar y prevenir amenazas de ciberseguridad.

En 2015, tanto los Estados Unidos como Europa adoptaron leyes relacionadas con la divulgación de información por parte de entidades corporativas y entre agencias gubernamentales con fines de ciberseguridad.

En el mismo mes en que se aprobó CISA, la Unión Europea llegó a un acuerdo sobre la Directiva de Seguridad de Redes e Información (NIS). En ella no solo se exige el establecimiento de estrategias nacionales de ciberseguridad, sino que se imponen obligaciones a los operadores de servicios esenciales (ej. servicios de transporte o servicios financieros) y a los proveedores de servicios digitales para que informen los incidentes de ciberseguridad a las autoridades nacionales.

Estas dos iniciativas señalan una era de regulación con respecto a las obligaciones de informar y responder a incidentes de ciberseguridad.

Estas dos iniciativas señalan una era de regulación con respecto a las obligaciones de informar y responder a incidentes de ciberseguridad.

TRANSFERENCIA TRANSFRONTERIZA DE DATOS

Un último aspecto de las políticas públicas relacionado con la coherencia del intercambio de información tiene que ver con la transferencia transfronteriza de datos personales para fines policiales y de inteligencia. Esta es un área cada vez más problemática y compleja en el ámbito de la seguridad nacional y el orden público. Tradicionalmente, la policía y las agencias de inteligencia podían acceder a cualquier dato personal en poder de empresas privadas (particularmente, en lo que respecta a las comunicaciones) con relativa facilidad debido a que esas empresas tenían su casa matriz en su jurisdicción. Hoy en día una gran mayoría de personas usan servicios de comunicaciones que se encuentran en el extranjero, particularmente, en los Estados Unidos.

Para ejecutar órdenes judiciales que requieran acceso a datos personales en manos de empresas, los Estados ahora dependen de diversos **tratados de asistencia legal recíproca** (**MLAT**), así como de pactos de intercambio de información como el Acuerdo de los Cinco Ojos (véase siguiente recuadro). Esto no solo entorpece las investigaciones, ya que la mayoría de las solicitudes realizadas a través del proceso de los **MLAT** pueden tardar casi un año, sino que crea incentivos para que los Estados eviten dichos procesos mediante la interceptación y otras técnicas de vigilancia.

EL ACUERDO DE LOS CINCO OJOS

Mientras que las fuerzas policiales generalmente tienen que pasar por procesos legales formales –y a menudo difíciles de manejar– para obtener y compartir información de otras fuerzas policiales de todo el mundo, los organismos de inteligencia suelen tener una relación mucho más fluida e integrada con sus homólogos extranjeros. Esto es particularmente cierto en el caso de las agencias de espionaje de los Estados Unidos, el Reino Unido, Australia, Nueva Zelanda y Canadá, que operan en una alianza conocida como los Cinco Ojos.

Respaldados por una serie de memorandos de entendimiento multilaterales y bilaterales que comenzaron en 1946, conocidos colectivamente como el Acuerdo de los Cinco Ojos (*Five Eyes Agreement*), las agencias de inteligencia de estos cinco países operan de manera altamente integrada, compartiendo datos en bruto de vigilancia, realizando operaciones conjuntas de espionaje y piratería, e incluso manteniendo personal en las instalaciones de cada uno de ellos.

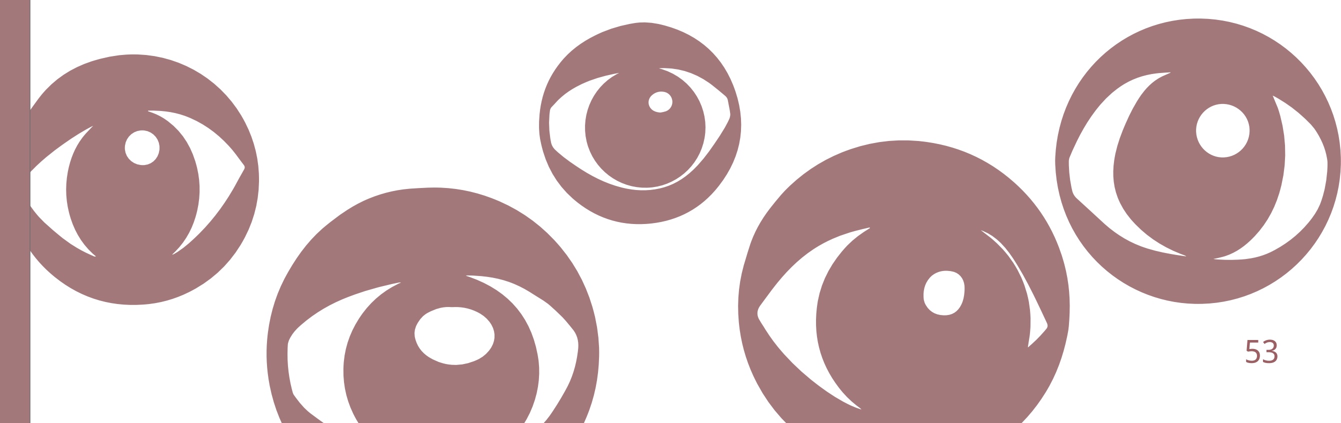
Con la publicación de documentos filtrados por el antiguo contratista de la Agencia Nacional de Seguridad o *National Security Agency* (NSA) de los Estados Unidos, Edward Snowden, el Acuerdo de los Cinco Ojos ha sido sometido a un mayor escrutinio. Sin embargo, el intercambio de información de inteligencia se mantiene en secretismo y alejado del escrutinio público. Organizaciones como Privacy International han pedido en repetidas ocasiones que se revelen públicamente todos los acuerdos de intercambio de inteligencia, no solo el Acuerdo de los Cinco Ojos, sino de alianzas similares en todo el mundo.

El Convenio del Consejo de Europa sobre el Ciberdelito (Convenio de Budapest, consulte la página 65) contiene disposiciones que permiten a las partes obtener acceso transfronterizo a datos informáticos almacenados, bien sea con consentimiento o cuando estén disponibles al público (artículo 32). La disposición está diseñada para permitir el acceso unilateral de una parte a datos personales que se encuentran en la jurisdicción de la otra parte, por lo tanto, constituye una manera de evitar los procesos de los **MLAT**. La cuestión del acceso transfronterizo es increíblemente polémica, entre otras cosas, porque el Artículo 32 puede interpretarse como un método que permite la requisa e incautación remota (también conocida como intrusión o ***hacking***), y Estados como Rusia la calificaron como una razón para no adherirse al Convenio, con el argumento de que viola el principio de soberanía.

En 2013, el Consejo de Europa propuso un Protocolo Adicional al Convenio, pero luego concluyó que dicha propuesta no sería factible. En los meses intermedios, se publicaron las revelaciones de Snowden sobre la vigilancia de los Estados Unidos y el Reino Unido, que transformaron el debate sobre el acceso de las agencias del orden público y de inteligencia a los datos personales. Un informe de 2013 del subgrupo del Comité del Convenio afirmó que los nuevos acontecimientos también obligaron a modificar el alcance del Artículo 32b, señalando que

> *las prácticas actuales con respecto al acceso directo de las agencias del orden público a los datos [...] con frecuencia van más allá de las posibilidades limitadas previstas en el Artículo 32b y en el Convenio de Budapest en general.*

Lo anterior plantea riesgos para los derechos humanos.



CAPACIDAD DE GESTIÓN, RESPUESTA Y COORDINACIÓN DE INCIDENTES; CERT Y CSIRT

Una última prioridad política en el campo de la seguridad de la información es construir la capacidad de los actores públicos y privados para gestionar y responder a los incidentes de ciberseguridad. Ya que la ciberseguridad no respeta fronteras, **interesa a todos los Estados apoyar el desarrollo de capacidades al interior de otros gobiernos para detectar y responder a las amenazas de ciberseguridad**. Los principales actores que dedican recursos a la creación de capacidades son los **CERT/CSIRT**, organizaciones internacionales como la UIT, organizaciones regionales como la OEA y la Unión de Telecomunicaciones del Commonwealth (CTU), así como grandes donantes de ayuda externa como los Estados Unidos y el Reino Unido.

COORDINACIÓN EN EL CIBERESPACIO: EL REINO UNIDO Y LOS ESTADOS UNIDOS RESPONDEN A LA RED DE BOTS *GAMEOVER* ZEUS

Responder a los ciberataques es un reto incluso para los organismos policiales mejor equipados del mundo. Los Estados Unidos y el Reino Unido fueron víctima de un ataque de *GameOver Zeus*, una red de computadores utilizada para robar millones de dólares de personas en todo el mundo. Aunque una impresionante coordinación condujo a la detección de la red de bots, la forma en la que la información fue divulgada al público fue problemática.

Tras la identificación de la red de bots, la Agencia Nacional Británica contra el Crimen o el *British National Crime Agency* (NCA) publicó un comunicado de prensa en el que instaba a la gente a tomar medidas para "protegerse contra el potente *software* malicioso". No estaba claro qué "pasos" debía dar la gente, más allá de visitar el sitio web *Get Safe Online*. Cuando el sitio web se cayó –posiblemente por el peso del tráfico– se produjo el caos.



El CERT del Reino Unido se sumó al pánico al volver a emitir la advertencia de la NCA, alentando a la gente a usar herramientas antivirus y antimalware, y a cambiar sus contraseñas. En ningún momento el CERT informó al público que solo el sistema operativo Windows fue afectado. Tampoco se publicó información posteriormente.

Fuente: http://www.bbc.com/news/technology-27681996

La construcción de capacidades de ciberseguridad es un ámbito alrededor del que abunda la cooperación, especialmente, a nivel regional. La Asamblea General de la OEA, por ejemplo, aprobó en 2004 la Resolución sobre la adopción de una estrategia interamericana integral de seguridad cibernética, que instó a los Estados miembros a implementar estrategias y a conformar y poner en funcionamiento grupos nacionales de "vigilancia y alerta", haciendo referencia a los **CERT.** La Directiva de la Unión Europea sobre seguridad de las redes y de la información requiere que los Estados miembros adopten estrategias nacionales de ciberseguridad que definan los objetivos estratégicos, y las medidas políticas y reglamentarias adecuadas en relación con este campo. También ordena que los Estados miembros designen una autoridad nacional competente para la implementación y aplicación de la Directiva, así como equipos de respuesta a incidentes de ciberseguridad (**CSIRT**) responsables del manejo de incidentes y riesgos. La Unión Europea, además, realiza capacitaciones de emergencia y organiza jornadas de sensibilización sobre la ciberseguridad en toda la UE.

Además de la construcción de capacidades a nivel internacional, los programas nacionales de educación y sensibilización pública son esenciales para educar a las personas sobre la ciberseguridad. Iniciativas como el programa *Get Cyber Safe* de Canadá, el sitio web *Cybersmart* de Australia y *EnTIConfío* de Colombia están diseñados para aumentar la conciencia general sobre el impacto y los orígenes de las amenazas de ciberseguridad.

... los programas nacionales de educación y sensibilización pública son esenciales para educar a las personas sobre la ciberseguridad.



INCORPORAR DERECHOS HUMANOS A LAS POLITÍCAS SOBRE SEGURIDAD DE LA INFORMACIÓN

La participación en la formulación de políticas de seguridad de la información está necesariamente restringida debido al carácter a menudo altamente técnico de los problemas. Sin embargo, hay mucho que las personas defensoras de derechos humanos pueden hacer para garantizar que estos se incorporen a dichas deliberaciones.



SUPERVISAR Y TRABAJAR CON LAS SDO PARA ASEGURARSE DE QUE PERMANEZCAN NEUTRALES Y NO SE POLITICEN DE UNA MANERA QUE PONGA EN RIESGO LOS DERECHOS HUMANOS

La existencia de normas técnicas para la ciberseguridad es congruente con la protección de los derechos a la privacidad, la libertad de expresión y la seguridad. Para asegurar que estas normas respeten los derechos, es vital que la sociedad civil supervise y dialogue con las SDO.

Hay varias formas de hacerlo. A nivel organizativo, la sociedad civil puede asistir a reuniones de las SDO, incluir las preocupaciones de derechos humanos en la agenda y proporcionar material educativo a quienes participan, destacando los vínculos entre el desarrollo de normas técnicas y los derechos humanos. El Grupo de Investigación de Consideraciones sobre el Protocolo de Derechos Humanos del IETF y el Grupo de Trabajo Intercomunitario de la ICANN sobre Responsabilidad Social y Empresarial de Respetar los Derechos Humanos son ejemplos de espacios en los que la sociedad civil puede participar.

Donde no existan oportunidades formales de participación a nivel organizativo, la sociedad civil también puede acudir a miembros individuales de las SDO. En una SDO de gran envergadura, como la Organización Internacional de Estandarización (ISO), esto significa acudir a la organización representativa nacional del país respectivo del grupo de la sociedad civil.

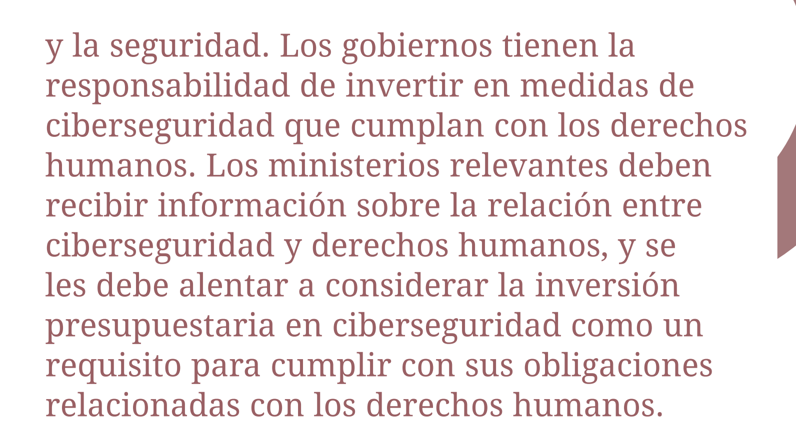
Las directivas de las SDO pueden tener una fuerte influencia sobre la posición que adopte las SDO por medio de normas específicas. Por lo tanto, la sociedad civil debe supervisar los nombramientos para garantizar que no comprometan la independencia de las SDO, por ejemplo, si un país en particular los postula por razones estratégicas. Las personas candidatas a cargos de liderazgo en las SDO deben tener los antecedentes técnicos necesarios y demostrar una comprensión clara de las implicaciones del desarrollo de normas de ciberseguridad en los derechos humanos.




ABOGAR POR LA PROVISIÓN DE RECURSOS ADECUADOS A ENTIDADES PÚBLICAS Y PRIVADAS PARA ASEGURAR QUE PUEDAN ADOPTAR Y CUMPLIR CON LAS NORMAS TÉCNICAS QUE PROVEAN EL MÁS ALTO NIVEL DE SEGURIDAD DE LA INFORMACIÓN

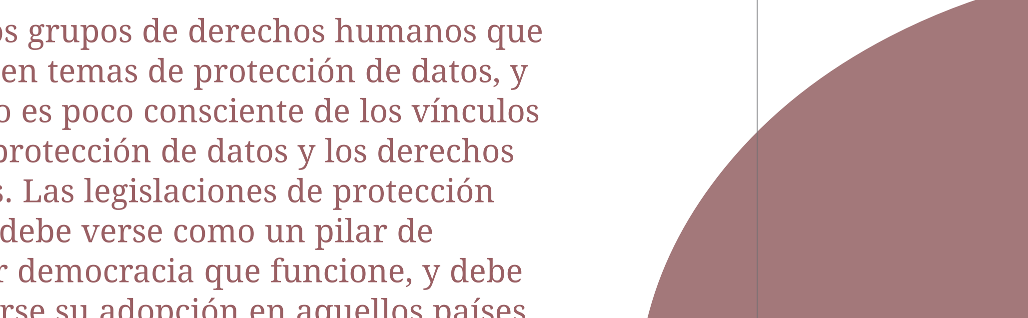
Las medidas que promuevan la ciberseguridad deben verse como parte de las obligaciones de un Estado de proporcionar las condiciones para el disfrute de los derechos a la privacidad, la libertad de expresión



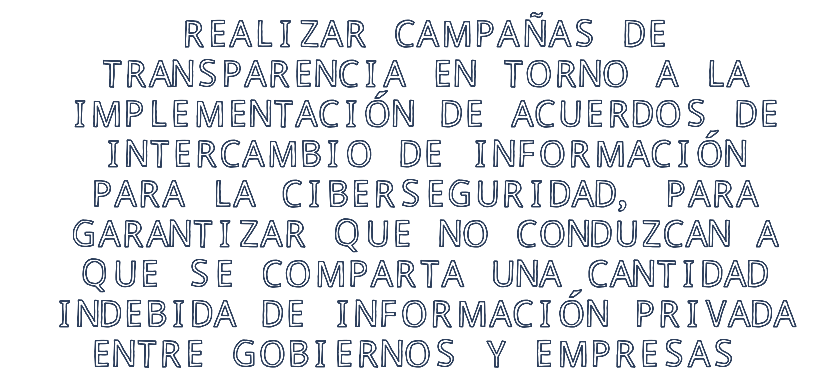


y la seguridad. Los gobiernos tienen la responsabilidad de invertir en medidas de ciberseguridad que cumplan con los derechos humanos. Los ministerios relevantes deben recibir información sobre la relación entre ciberseguridad y derechos humanos, y se les debe alentar a considerar la inversión presupuestaria en ciberseguridad como un requisito para cumplir con sus obligaciones relacionadas con los derechos humanos.

3 ABOGAR POR UNA LEGISLACIÓN SÓLIDA DE PROTECCIÓN DE DATOS Y PRIVACIDAD EN TODO EL MUNDO



Hay pocos grupos de derechos humanos que trabajan en temas de protección de datos, y el público es poco consciente de los vínculos entre la protección de datos y los derechos humanos. Las legislaciones de protección de datos debe verse como un pilar de cualquier democracia que funcione, y debe promoverse su adopción en aquellos países que no cuentan aún con una ley de este tipo, como India, China, los Estados Unidos, Cuba, Guatemala, Paraguay y la mayoría de los países africanos. Donde exista una ley de protección de datos, la sociedad civil debe buscar que sea adecuada para hacer frente a la amplia gama de problemas existentes de seguridad de la información.



4 REALIZAR CAMPAÑAS DE TRANSPARENCIA EN TORNO A LA IMPLEMENTACIÓN DE ACUERDOS DE INTERCAMBIO DE INFORMACIÓN PARA LA CIBERSEGURIDAD, PARA GARANTIZAR QUE NO CONDUZCAN A QUE SE COMPARTA UNA CANTIDAD INDEBIDA DE INFORMACIÓN PRIVADA ENTRE GOBIERNOS Y EMPRESAS

Cada vez más, los gobiernos están adoptando leyes que requieren la divulgación de información sobre ciberamenazas del sector privado. Se debe corregir la falta de transparencia en torno a dicha cooperación, realizada bajo los auspicios de la seguridad nacional y la ciberseguridad; solo a través del escrutinio público, los gobiernos y las empresas rendirán cuentas a la ciudadanía. Las personas defensoras de derechos humanos deben hacer campaña para que los gobiernos y las empresas publiquen detalles sobre la cantidad y el tipo de información que se comparte en virtud de los acuerdos de intercambio de información por razones de ciberseguridad.

5 SUPERVISAR LA NEGOCIACIÓN DE ACUERDOS DE INTERCAMBIO TRANSFRONTERIZO DE DATOS PARA EVITAR EL DETERIORO DE LAS SALVAGUARDAS DE LOS DERECHOS HUMANOS

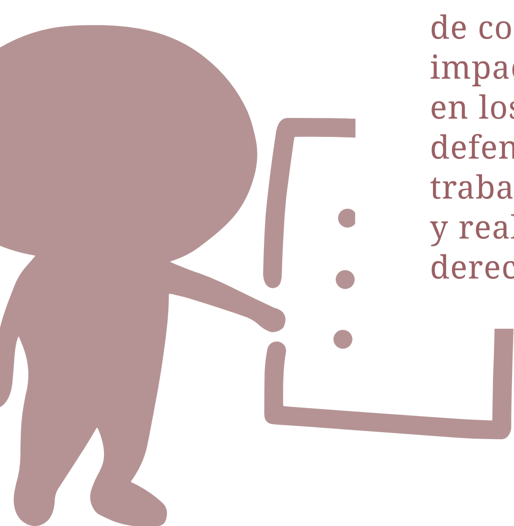
Las personas defensoras de derechos humanos deben exigir que las negociaciones en torno a los acuerdos de intercambio transfronterizo

de datos sean tan públicas como sea posible para garantizar que no sacrifiquen las protecciones a los derechos humanos a cambio de mayores poderes de vigilancia. Es común que exista un grado extremo de secreto en torno a tales acuerdos. En estos casos, las leyes de acceso a la información, así como las campañas públicas, deben utilizarse para orientar la incidencia de la sociedad civil.



6 ABOGAR POR LA INCLUSIÓN DE LOS DERECHOS HUMANOS EN EL CORAZÓN DE TODAS LAS INICIATIVAS DE CREACIÓN DE CAPACIDADES DE CIBERSEGURIDAD

Los derechos humanos no deberían ser una cuestión secundaria o de simple cumplimiento: deberían colocarse desde el principio en el centro de la formación en ciberseguridad. Las instituciones y los gobiernos donantes que participan en iniciativas de creación de capacidad en el extranjero tienen la responsabilidad de compartir el conocimiento sobre el impacto de las medidas de ciberseguridad en los derechos humanos. Las personas defensoras de derechos humanos podrían trabajar con estos actores para diseñar y realizar capacitación y educación en derechos humanos.





LA CIBERSEGURIDAD COMO CIBERDELITO

¿Sigue siendo seguro salir?

Es difícil imaginar un delito moderno que no implique, en algún momento de su ejecución, el uso de un computador. Según la definición de delitos informáticos (delitos que involucran computadores y redes), todos, desde un pequeño narcotraficante que envía mensajes a sus clientes usando WhatsApp, a un ladrón de arte que usa Google Maps para trazar su ruta de escape, están implicados en un ciberdelito.

La mayoría de la gente probablemente no consideraría los delitos tradicionales que utilizan internet como ciberdelitos. Para la persona promedio, los ciberdelitos son hechos punibles que solo pueden ocurrir en línea, por ejemplo, el robo de datos de identidad o el uso de ***ransomware***. Sin embargo, el discurso sobre el ciberdelito con frecuencia desdibuja la línea entre estos dos aspectos del derecho.

Le resultaría difícil a quienes redactaron la primera ley mundial de delitos informáticos, el Convenio de Budapest, prever que el ciberdelito podría llegar a significar "todo delito". Después de todo era 2001: los teléfonos inteligentes apenas se habían inventado y nadie podría haber predicho hasta qué punto los computadores se integrarían tan profundamente en nuestras vidas, que algún día cabrían en nuestras manos, reemplazarían nuestros relojes y televisores, e incluso conducirían nuestros vehículos.

Es difícil imaginar un delito moderno que no implique, en algún momento de su ejecución, el uso de un computador.

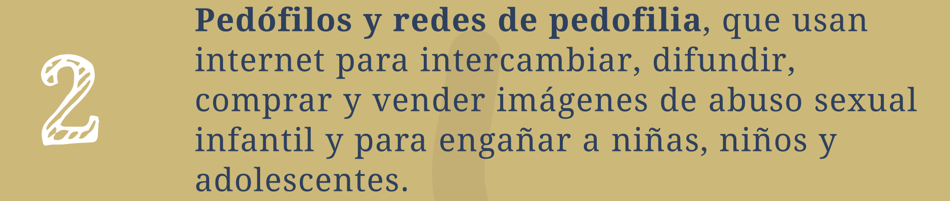
Hoy en día, además de la ciberseguridad, el ciberdelito se encuentra en el centro de los debates políticos sobre la regulación de internet, la seguridad infantil, la vigilancia gubernamental, la vigilancia policial y la lucha contra el terrorismo.

Cuatro tipos de delincuentes dominan las discusiones sobre la formulación de políticas públicas sobre ciberdelitos:

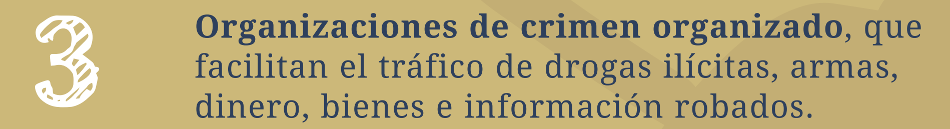


Grupos terroristas, cuyo uso de internet va desde lo básico (uso de redes sociales para difundir material de reclutamiento, uso de aplicaciones de mensajería para comunicarse) hasta lo sofisticado (uso de enrutamiento y alojamiento anónimos y de sitios web para la planificación, el reclutamiento y la difusión de materiales).





2 **Pedófilos y redes de pedofilia**, que usan internet para intercambiar, difundir, comprar y vender imágenes de abuso sexual infantil y para engañar a niñas, niños y adolescentes.



3 **Organizaciones de crimen organizado**, que facilitan el tráfico de drogas ilícitas, armas, dinero, bienes e información robados.

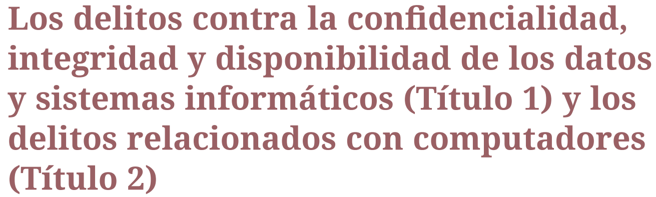
4 **Ciberagresores y hackers**, que atacan la información y las redes para adquirir, eliminar o alterar información, causar daños y debilitar la seguridad.

EL PROPÓSITO DE LAS LEYES CONTRA EL CIBERDELITO

Aunque la definición de ciberdelito es lo suficientemente amplia como para extenderse a otros delitos más mundanos que ocurren fuera de internet, las categorías mencionadas anteriormente son las que aparecen con mayor frecuencia en relación con las medidas de ciberseguridad. Sin embargo, las leyes contra el ciberdelito, generalmente, tienen una aplicación más limitada a los delitos de uso indebido de computadores, fraude y abuso (aquellos que involucran ciberagresores y hackers) y los delitos relacionados con los contenidos.

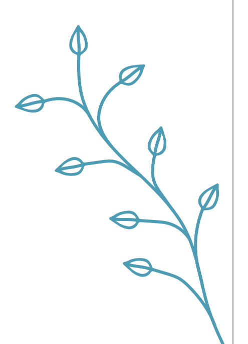
CONVENIO DE BUDAPEST

El Convenio de Budapest es la ley autorizada sobre delitos informáticos y el fundamento de las legislaciones de los Estados que hacen parte de este tratado. Hay tres categorías sustantivas de delito:



1

Los delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos (Título 1) y los delitos relacionados con computadores (Título 2)
Estos son aquellos delitos principalmente relacionados con **ciberataques** y ***hacking***, e incluyen la interferencia e interceptación de datos. Muchos países han incorporado dichas disposiciones en el ámbito de la legislación sobre “uso indebido de computadores” o “sistemas informáticos”.





Delitos relacionados con los contenidos (Título 3)
Estos delitos se relacionan con la difusión de “pornografía infantil”. El uso de la palabra “pornografía” ha sido muy controvertida y muchos Estados ahora se refieren a “imágenes de abuso sexual infantil” o “material de pedofilia”.



Delitos relacionados con la infracciones al derecho de autor (Título 4)
Estos delitos se refieren a violaciones al derecho de autor a escala comercial mediante un sistema informático.

El Convenio describe una serie de requisitos procedimentales para facilitar la investigación del ciberdelito y la obtención de pruebas. Estos incluyen disposiciones generales sobre la extradición y la asistencia judicial recíproca, así como la obligación de legislar para otorgar facultades que obligan a:

la conservación expedita de datos informáticos almacenados (Artículo 16), y la conservación y divulgación de datos de tráfico (Artículo 17);

la producción de datos informáticos específicos por parte de quienes los poseen (a saber, empresas de internet y proveedores de telecomunicaciones), específicamente información de personas suscriptoras y **metadatos** (Artículo 18);

el allanamiento e incautación de datos almacenados (Artículo 19);

la recolección en tiempo real de datos de tráfico (Artículo 20); y

la interceptación de datos de contenido (Artículo 21).

PROTOCOLO ADICIONAL SOBRE ACTOS RACISTAS Y XENÓFOBOS

Los delitos relacionados con el contenido del Convenio de Budapest se complementaron posteriormente en 2006 con la adopción de un Protocolo Adicional, que aborda el uso de internet (o “sistemas informáticos”) para propagar material racista o xenófobo. Específicamente, el Protocolo Adicional requiere que las partes promulguen leyes que tipifiquen los siguientes delitos:



distribuir o poner a disposición del público material racista y xenófobo a través de un sistema informático (Artículo 3);

amenazar, a través de un sistema informático, con la comisión de un delito grave como lo define su legislación nacional, o insultar, a través de un sistema informático, a personas por motivo de su pertenencia a un grupo, que se distingue por raza, color, ascendencia, nacionalidad u origen étnico, así como la religión, si se utiliza como pretexto para cualquiera de estos factores (Artículo 4); y

distribuir o poner a disposición del público, a través de un sistema informático, material que niega, minimiza crasamente, aprueba o justifica actos que constituyan genocidio o crímenes de lesa humanidad (Artículo 6).

Hasta la fecha, alrededor de 32 Estados han ratificado el Protocolo Adicional (todos miembros del Consejo de Europa, con excepción de 3 Estados: Marruecos, Paraguay y Senegal). Estados Unidos, que no es parte del Consejo de Europa, pero es miembro del Convenio de Budapest, se ha negado a adoptar el Protocolo, señalando que las disposiciones son contrarias a sus protecciones constitucionales. De hecho, el Protocolo Adicional plantea serias preocupaciones sobre el umbral a partir del cual el discurso legítimo en línea se convierte en discurso de odio, que se puede limitar legítimamente en la legislación de derechos humanos.

EL CONVENIO Y LAS LEGISLACIONES NACIONALES SOBRE LOS CIBERDELITOS

Durante la redacción del Convenio, se planteó la preocupación de que podría utilizarse para contravenir los derechos humanos. Con su transposición a las legislaciones nacionales, se ha demostrado que estas preocupaciones estaban justificadas. En varios casos, el Protocolo Adicional se ha utilizado como modelo para incluir disposiciones abarcadoras que penaliza el contenido y otras actividades en línea. Algunos ejemplos incluyen:

La Ley de Delitos Cibernéticos de Kuwait, aprobada en 2015, contiene disposiciones que imponen penas de prisión y multas por insultar a la religión o a figuras religiosas, y por criticar al Emir por internet (Artículo 6); prohíbe las declaraciones por internet que puedan ser crítica al sistema judicial o perjudicar las relaciones de Kuwait con otros Estados, o que publiquen información clasificada, sin excepciones para divulgaciones de interés público (Artículo 6); e impone una pena de hasta 10 años de prisión por usar internet para “derrocar al régimen gobernante del país cuando esta instigación incluya una incitación a cambiar el sistema por la fuerza o por medios ilegales, o instando al uso de la la fuerza para cambiar el sistema social y económico que existe en el país, o para adoptar credos que tengan como objetivo destruir los estatutos básicos de Kuwait por medios ilegales” (Artículo 7).

La Convención de la Unión Africana sobre ciberdelitos y protección de datos, adoptada en 2014, tipifica como delito la creación, difusión o descarga de contenido que contenga amenazas o insultos por motivos de raza, color, ascendencia, origen nacional o étnico, o religión, así como la participación en grupos físicos o en línea “establecidos con miras a preparar o cometer” un delito incluido en este tratado.



La Ley contra el Ciberdelito de Arabia Saudí incluye una referencia a la “protección del interés público, la moral y los valores comunes” y se ha utilizado contra personas blogueras y otras por delitos relacionados con

insultar al funcionariado públicos o apoyar a fuerzas distintas al gobierno actual.

La Ley de Ciberdelitos de Tanzania, promulgada en mayo de 2015, penaliza a "cualquier persona que publique información, datos o hechos presentados en una imagen, texto, símbolo o cualquier otra forma en un sistema informático donde dicha información, datos o hechos sean falsos, engañosos o inexactos" (Sección 16).

La Ley de Prevención de Delitos Electrónicos de Pakistán, aprobada en 2016, criminaliza a cualquier persona que "prepare o difunda" cualquier tipo de comunicación electrónica con la intención de "fomentar el odio interreligioso, sectario o racial" (Artículo 11). La legislación también contiene un delito de "ciberterrorismo", que incluye la "glorificación" del delito o el acceso no autorizado, la copia o la transmisión de información "crítica" con la intención de crear un ánimo de miedo o inseguridad en el gobierno o el público, o para promover el odio religioso, étnico o sectario (Artículo 10). Además, crea amplias facultades de vigilancia y adquisición de datos, y poderes de censura de contenido por parte del gobierno cuando este lo considere "necesario en interés de la gloria del Islam o la integridad, seguridad o defensa de Pakistán" (Artículos 35-37).

La posibilidad de que se utilice el ciberdelito para promover leyes que restrinjan la libertad de expresión, los comentarios políticos y la crítica genuina es, sin duda, el aspecto más preocupante del discurso sobre ciberdelito.

Al redactar legislaciones sobre ciberdelitos, que requieren conocimientos especializados y experiencia, los países pueden recurrir a "leyes modelo". Sin embargo, el uso de estos modelos puede ser problemático. Un estudio encargado por el Consejo de Europa, sobre leyes modelo de ciberdelito (véase más en "Recursos Seleccionados") concluyó que

> *el uso de tales leyes modelo plantea riesgos y preocupaciones graves. La ausencia de disposiciones esenciales, lenguaje defectuoso [...] y su divergencia e incongruencia con las mejores prácticas internacionales perjudican el objetivo de lograr una mayor cooperación internacional contra el delito cibernético.*

PERSONAS DEFENSORAS DE DERECHOS HUMANOS LUCHAN CONTRA LA "LEY CIBERMARCIAL" EN FILIPINAS



En 2012, el Gobierno filipino aprobó la Ley de Prevención de la Ciberdelincuencia. Grupos feministas, personas defensoras de derechos humanos y periodistas criticaron fuertemente esta legislación por sus amplias disposiciones que penalizaban todo, desde el cibersexo hasta la difamación. Las ONG se unieron para establecer la Alianza Filipina para la Libertad de Internet, organizaron protestas callejeras y presentaron peticiones ante el Tribunal Supremo.

El Tribunal Supremo filipino emitió y luego prorrogó interdictos temporales contra la aplicación de la ley hasta que el caso fue resuelto en febrero de 2014. En ese momento, el Tribunal confirmó la disposición relativa a la difamación en línea, pero limitó su aplicación a los casos en que se refiere a personas distintas del autor original. Las personas destinatarias y usuarias de internet que reaccionen a un mensaje potencialmente difamatorio no estarán cubiertas por la difamación en línea.

El Tribunal anuló la Sección 4(c)(3) (sobre comunicaciones comerciales no solicitadas), la Sección 12 (recogida de datos de tráfico en tiempo real) y la Sección 19 (restricción o bloqueo de datos informáticos).

La acción policial contra el ciberdelito se está convirtiendo en sinónimo de represión del cuestionamiento del *statu quo*. Esto menoscaba la eficacia y la libre actuación de las personas defensoras de derechos humanos.

Existe un amplio debate en el ámbito del ciberdelito en torno a la necesidad de promulgar leyes de delitos informáticos que abarquen actividades sin límites jurisdiccionales.

Actualmente, debido al limitado alcance del Convenio de Budapest, las legislaciones sobre ciberdelitos no están armonizadas a nivel mundial. Lo que plantea un problema para los Estados que buscan combatir infracciones como el uso indebido de sistemas informáticos, ***hacking*** y **ciberataques** – cuando, por ejemplo, se origina en un país que no lo criminaliza, dificultando o imposibilitando la posibilidad de procesar a los responsables.

Sin embargo, estos debates sobre armonización, rápidamente, suelen derivar en la necesidad de ajustar las facultades de las autoridades del orden público y de inteligencia para llevar a cabo tareas de vigilancia, de monitoreo de actividades en línea, de bloqueo y filtrado de contenidos de internet, y de represión contra el uso de las herramientas de anonimización.

Otro ejemplo del control que puede ejercerse con la legislación sobre cibercrimen se empieza a gestar en el seno de la ONU. A finales de 2019, la Asamblea General aprobó una resolución auspiciada por Rusia y respaldada por China, Cuba, Corea del Norte, Nicaragua, Siria, Venezuela y otros 39 países, que tiene por objeto establecer un grupo para examinar y crear una convención para prevenir el ciberdelito. Sin embargo, la resolución es tan imprecisa que podría conducir a la penalización de actividades cotidianas en línea en las que confían periodistas, grupos de derechos humanos y otros miembros de la sociedad civil, como el uso de aplicaciones de mensajería cifradas. También podría dar amplios poderes a los gobiernos para bloquear sitios web considerados críticos con las autoridades, o incluso redes, aplicaciones y servicios enteros que faciliten el intercambio y el acceso a la información en línea. El texto de la resolución aprobada, además, parece alinearse con la Ley de una Internet Soberana promulgada en 2019 en Rusia, que, en teoría, permitirá al Kremlin desconectar su internet del resto del mundo. Lo que demuestra las tensiones que existen entre los países por impulsar sus modelos regulatorios y prácticas de control del ciberespacio.

BORRADOR DEL SEGUNDO PROTOCOLO ADICIONAL

En septiembre de 2017, el Consejo de Europa se comprometió a preparar un segundo protocolo adicional al Convenio de Budapest. Su objetivo es establecer disposiciones para un régimen de asistencia judicial recíproca más eficaz y simplificado que los **MLAT**, que permita la cooperación directa con los proveedores de servicios de otros Estados partes en el Convenio y la ampliación de las búsquedas transfronterizas.

Sin embargo, un grupo amplio de organizaciones de la sociedad civil ha llamado la atención sobre los riesgos que se corren con la actual propuesta. Resaltan que no incluye mecanismos de evaluación de derechos humanos que son inherentes al actual sistema de **MLAT** que se usa, entre otras, para sortear conflictos en materia de derechos fundamentales y salvaguardas legales que surgen entre los países. Además, denuncian que la propuesta establecería normas que están por debajo de los estándares mínimos de derechos humanos establecidos en la jurisprudencia internacional. Por último, dan aviso sobre los pocos límites sustanciales para que las reformas legales en cada país que requeriría este protocolo incluya suficientes garantías para que no violen los derechos humanos en el acceso transfronterizo de datos.



VIGILANCIA MASIVA

Esto dijo en noviembre de 2015 la entonces Secretaria de Interior británica, Theresa May, cuando presentó el proyecto de ley de facultades de investigación, que contiene poderes de **vigilancia masiva** y retención generalizada de datos.

Pero una sociedad digital también nos plantea desafíos. Los mismos beneficios que disfrutamos todas las personas están siendo atacados por criminales serios y organizados, estafadores en línea y terroristas.
La amenaza es clara [... l]a frecuencia y el costo de los ciberataques está aumentando, ya que el 90% de las grandes organizaciones sufrieron una violación a la seguridad de la información el año pasado. Y el Comando contra la Explotación Infantil y Protección en Línea estima que hay 50,000 personas en este país que descargan imágenes indecentes de niñas, niños y adolescentes.
El trabajo de las agencias policiales, de seguridad y de inteligencia se ha vuelto mucho más difícil en esta era digital. Por lo tanto, es correcto que quienes se encargan de protegernos tengan las facultades necesarias para hacerlo.

El entonces Ministro del Interior francés, Bernard Cazeneuve, habló en julio de 2015 sobre la *Loi sur le Renseignement*, la ley francesa de inteligencia que contiene poderes de **vigilancia masiva** y de retención generalizada de datos.

La ley de inteligencia [...] reforzará la eficacia de nuestras medidas preventivas. Estamos mejorando los medios de nuestro servicio, incluida la creación de 1,500 empleos desde enero [...] Estos empleos se distribuirán entre inteligencia extranjera y nacional, y la lucha contra el ciberdelito.

Cada vez más, y especialmente bajo la bandera de la lucha contra el ciberdelito, los Estados están desarrollando y expandiendo programas de vigilancia masiva que incluyen la recopilación y el análisis generalizado de información privada.

Pocas cuestiones de derechos humanos han atraído tanto debate público y atención política en los últimos años como la vigilancia estatal y el papel del sector privado para facilitarla. Más que quizás cualquier otra comunidad, las personas defensoras de derechos humanos entienden la expansión gradual de la vigilancia estatal en línea y sus efectos no solo para la privacidad, sino también para su capacidad de expresarse y organizarse con confianza y sin temor.

Cada vez más, y especialmente bajo la bandera de la lucha contra el ciberdelito, los Estados están desarrollando y expandiendo programas de vigilancia masiva que incluyen la recopilación y el análisis generalizado de información privada. Hay dos tipos de **vigilancia masiva** que dominan las polémicas actuales sobre políticas públicas y los debates legislativos: la interceptación masiva y la retención obligatoria de datos de comunicaciones.

La creciente popularidad de la **vigilancia masiva** entre los gobiernos de todo el mundo se puede atribuir a una serie de factores, entre ellos:

la rápida disminución del costo de la tecnología y el almacenamiento de datos, lo que hace que la captura y el almacenamiento (incluso de forma indefinida) de los datos sean más baratos que nunca;

la ubicuidad de los dispositivos digitales, que generan y transmiten grandes cantidades de información que se pueden adquirir

y analizar fácilmente para rastrear y monitorear a personas nacionales y extranjeras; y

el poder de procesamiento de la informática, que ahora puede analizar, procesar y obtener información de grandes conjuntos de datos con un grado de precisión mucho mayor que en cualquier otro momento de la historia, lo que supuestamente reduce la necesidad del análisis humano de la inteligencia.

Por encima de todo, sin embargo, la clara preferencia por la **vigilancia masiva** está motivada por un cambio de mentalidad en cuanto a la naturaleza de la seguridad y el papel de la vigilancia. Como la ciberseguridad y la lucha contra el terrorismo transnacional se han convertido en los principales motores de la política de vigilancia, ha prosperado una conceptualización específica de la vigilancia moderna que predica que todos los actos de comunicaciones digitales son piezas potencialmente necesarias de un inmenso rompecabezas de seguridad, que solo se puede resolver si se recoge cada pieza. O, para usar una analogía más popular, que la aplicación efectiva de la ley y la protección de la ciberseguridad requieren encontrar agujas en un pajar, y la única manera de hacerlo es recolectando cada paja disponible.

Las capacidades de interceptación masiva son pieza clave de las capacidades de vigilancia, tanto existentes como propuestas, de varios países. Por ejemplo:

Desde 2008, la Sección 702 de la Ley de Vigilancia de Inteligencia Extranjera de los Estados Unidos ha facilitado la recolección masiva de las comunicaciones de personas no nacionales, lo que otorga protección legal a los sistemas de **vigilancia masiva** tales como *Upstream*. Los Estados Unidos también utiliza la Orden Ejecutiva 12333 para realizar una recolección masiva de datos enteramente extranjeros, aunque poco se sabe sobre este poder.

India aprobó la Ley de Tecnología de la Información de 2008, cuya Sección 89 permite al Gobierno interceptar, monitorear o descifrar todas las comunicaciones si es necesario o conveniente hacerlo en pro de la soberanía nacional o integridad territorial del país, entre otras razones de amplio alcance.

También en 2008, Suecia adoptó la Ley de Inteligencia de Señales (también conocida como Ley FRA) que permite la interceptación masiva de las comunicaciones por cable.



En 2013, Colombia adoptó una ley de inteligencia que amplió los poderes de las agencias de inteligencia para “monitorear” las comunicaciones en masa, sin autorización. Además, una normativa de 2012, obligó a los operadores de telecomunicaciones a crear **puertas traseras** para el acceso al tráfico y a los datos de comunicaciones por parte de la Fiscalía General. Se sabe que el país ha adquirido una serie de capacidades técnicas que permiten la interceptación masiva y la adquisición de datos.

La Ley de Poderes de Investigación del Reino Unido de 2016 reproduce los poderes de interceptación en masa de la Sección 8 de la Ley de Regulación de Poderes de Investigación de 2000, y también crea poderes para llevar a cabo ***hacking*** y adquisición de datos en masa.

En 2015, Francia aprobó dos leyes que abren la puerta a la **vigilancia masiva**: el *Loi du 24 juillet 2015 relative au Renseignement* que, entre otras cosas, autoriza la instalación de "cajas negras" en la infraestructura de los proveedores de telecomunicaciones para permitir el filtrado de contenido terrorista; y la Ley de Vigilancia Internacional, aprobada más tarde en 2015 después de haber sido separada de la ley anterior debido a preocupaciones constitucionales, que autoriza la interceptación masiva de comunicaciones extranjeras.

En 2015, Suiza introdujo una nueva ley de vigilancia que permite la interceptación de cables para fines de **vigilancia masiva**.

Los sistemas de interceptación masiva también se pueden comprar en el mercado privado. Por ejemplo, México es uno de los principales compradores de sofisticadas herramientas de vigilancia desarrolladas por compañías como *NSO Group* y *Hacking Team*, que se han utilizado contra periodistas, activistas y personas defensores de derechos humanos, sin mediar autorizaciones judiciales.

Las revelaciones de Snowden sobre los programas de interceptación masiva operados por los Estados Unidos y el Reino Unido llevaron al entonces Relator Especial de las Naciones Unidas sobre la protección de los derechos humanos en la lucha contra el terrorismo, Ben Emerson, a concluir que "la existencia misma de programas de **vigilancia masiva** constituye potencialmente una interferencia desproporcionada con el derecho a la privacidad". A pesar de esto, los Estados continúan sosteniendo que es una herramienta necesaria para combatir el terrorismo y el ciberdelito. Leyes nacionales actuales de países europeos han extendido los poderes de interceptación masiva de los organismos de inteligencia y seguridad. En el Reino Unido, por ejemplo, la Ley de Poderes de Investigación obliga a las empresas a entregar datos en masa de las comunicaciones a estas autoridades. En Países Bajos, la nueva Ley sobre Servicios de Inteligencia y Seguridad otorga a la agencia holandesa de inteligencia y a su contraparte militar, entre otras cosas, el poder de acceder y retener los **metadatos** de su ciudadanía.

La brecha cada vez mayor entre el derecho internacional y la práctica estatal plantea serias preocupaciones acerca de la protección de los derechos humanos, en un clima cada vez más orientado a la seguridad (consulte el recuadro sobre "Securitización" en la página 38). Al la vez que los Estados están ampliando sus poderes de vigilancia, una serie de organismos regionales e internacionales de derechos humanos ha declarado la no conformidad de las medidas de vigilancia e interceptación masiva con el derecho internacional de los derechos humanos, incluyendo:

El Alto Comisionado de las Naciones Unidas para los Derechos Humanos (A/HRC/27/37)

El Relator Especial de las Naciones Unidas sobre la protección de los derechos humanos en la lucha contra el terrorismo (A/69/397)



El Relator Especial de las Naciones Unidas sobre el derecho a la libertad de opinión y expresión. (A/HRC/23/40)

El Tribunal de Justicia de la Unión Europea (en *Schrems v. el Comisario de Protección de Datos de Irlanda*, sentencia de 6 de octubre de 2015)

El Tribunal Europeo de Derechos Humanos en dos sentencias de diciembre de 2015 (*Zakharov v. Rusia*) y enero de 2016 (*Szabo y Vissy v. Hungría*)

Los relatores especiales para la libertad de expresión de los organismos multilaterales internacional y regionales en la *Declaración conjunta sobre programas de vigilancia y su impacto para la libertad de expresión.*

La retención obligatoria de datos es otra forma de **vigilancia masiva**. Al obligar a los proveedores de servicios de comunicaciones a retener y, en ocasiones, generar información extensa sobre las comunicaciones, ubicaciones y conexiones de una persona, y poner esos datos a disposición de la policía y agencias de inteligencia cuando lo soliciten, las leyes de retención de datos constituyen una forma de vigilancia generalizada que impide el **anonimato** en línea e inhibe la libertad de expresión. También crea responsabilidades para que los proveedores de servicios eviten los ataques o sean responsables de la seguridad de los datos retenidos ante posibles ataques dirigidos, robos o alteración de los mismo.

EL COSTE DE LOS CIBERATAQUES

Una serie de ciberataques de alto nivel ha hecho que empresas y organizaciones sufran costos tanto financieros como de reputación:

* **Un hospital de Los Ángeles, el Hollywood Presbyterian Medical Centre, pagó 17,000 dólares en bitcoin a un grupo de hackers que tomaron el control de la red del hospital con un programa malicioso de rescate (*ransomware*).**

* **El proveedor británico de redes telefónicas TalkTalk perdió 101,000 clientes y 60 millones de libras esterlinas después de que se accediera a los detalles financieros de 156,000 de sus clientes en un ciberataque en 2015.**

* **Un ataque a Sony Pictures en 2014, supuestamente en respuesta a la decisión de la compañía de hacer la película de parodia norcoreana *The Interview*, puede no haber tenido graves consecuencias financieras para la compañía, pero causó una gran vergüenza para el personal de la compañía cuyos correos electrónicos y registros privados se hicieron públicos al mundo. Más de 3,000 números de Seguro Social del personal de la compañía fueron expuestos, junto con información salarial, evaluaciones laborales e historias clínicas.**

Las leyes europeas de retención de datos se originaron en el Reino Unido. En el año 2000, casi al mismo tiempo que se estaba negociando el Convenio de Budapest sobre el Ciberdelito, se intentó aprobar una ley que obligaba a conservar los datos durante siete años. Después de repetidos intentos fallidos de aprobar la legislación a través del Parlamento Europeo, se forzó su aprobación a través de la Directiva Europea de Retención de Datos cuando el Reino Unido ocupó la Presidencia de la UE en 2006. La retención obligatoria de datos se convirtió entonces en ley en toda Europa.

A raíz de las revelaciones de Snowden, y en particular del descubrimiento del programa de la NSA de recolección masiva de **metadatos** de telefonía, se prestó renovada atención a las implicaciones de la retención de datos a los derechos humanos. Demandas en los Estados Unidos, Canadá, el Reino Unido y el Tribunal de Justicia de la Unión Europea cuestionaron la presunción de que los **metadatos** no están protegidos por el derecho a la intimidad.

En el caso del Tribunal de Justicia de la Unión Europea de *Digital Rights Ireland v. Ireland* (2014), tras una demanda presentada por la ONG Digital Rights Ireland sobre la validez de la Directiva Europea de Retención de Datos, la Gran Sala observó los peligros de recopilar y utilizar datos personales en masa. Concluyó que la Directiva “implica una interferencia con los derechos fundamentales de prácticamente toda la población europea”. Se procedió a invalidar la ley por razones de proporcionalidad.

Después de las revelaciones de Snowden, el discurso político sobre la vigilancia masiva (tanto la interceptación masiva como la retención obligatoria de datos) se ha polarizado drásticamente.

La anulación de la Directiva Europea de Retención de Datos arrojó dudas sobre la base jurídica de la Unión Europea para exigir la retención de datos de las comunicaciones en los Estados miembros. A partir de esta decisión, muchos países europeos abandonaron los poderes de retención de datos, mientras que otros volvieron a legislar a su favor aunque con

ello puedan enfrentar nuevos cuestionamientos en los tribunales nacionales y regionales. En otras regiones del mundo, Australia adoptó leyes de retención de datos en marzo de 2015, mientras que el parlamento de Paraguay se resistió a promulgar las leyes de retención de datos propuestas en julio de 2015, una rara excepción. Después de una serie de casos judiciales relacionados con el programa de la NSA de recolección generalizada de **metadatos**, la Sección 215 de la Ley Patriota expiró en junio de 2015 y se modificó por medio de la *USA Freedom Act*, que altera, pero no elimina, los procesos de retención de **metadatos**.

Después de las revelaciones de Snowden, el discurso político sobre la **vigilancia masiva** (tanto la interceptación masiva como la retención obligatoria de datos) se ha polarizado drásticamente. Por un lado, los mecanismos y tribunales de derechos humanos declaran repetidamente su incompatibilidad con el marco legal de los derechos humanos. Por otro lado, los Estados, acaso envalentonados por las revelaciones de las personas alertadoras (*whistleblower*), continúan reforzando y ampliando sus capacidades de **vigilancia masiva** en nombre de la ciberseguridad y la prevención del terrorismo.

CIFRADO

El elemento más polémico y contradictorio de las políticas de ciberdelitos se relaciona con el **cifrado** y su supuesto rol como facilitador de hechos delictivos.

Las autoridades del orden público y entidades gubernamentales argumentan que el **cifrado** proporciona a los ciberdelincuentes y terroristas “espacios seguros” para esconderse de la detección de mecanismos de vigilancia estatales.

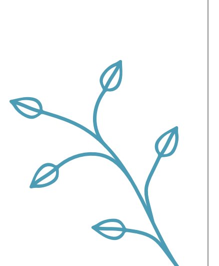
Al restringir el **cifrado** y exigir la creación de **puertas traseras** estatales se debilita la seguridad, especialmente la ciberseguridad, en lugar de fortalecerla. Menos **cifrado** significa más delitos en línea, ya que los ciberdelincuentes y ladrones de identidad pueden navegar las inseguridades de los servicios de correo electrónico y sitios web bancarios con mayor facilidad. Además, las **puertas traseras** (la solución propuesta para la proliferación creciente del **cifrado**), diseñadas ya sea para el uso por parte de un actor estatal o de uno privado en respuesta a, por ejemplo, una orden judicial, pueden ser fácilmente explotadas por otros actores estatales o no estatales. Una vez existe una **puerta trasera** es increíblemente difícil restringir quién podría acceder a ella.

No obstante, algunos Estados continúan argumentando que el **cifrado** plantea obstáculos insuperables a las actividades legítimas de las fuerzas del orden público, y han pedido la adopción de una legislación que prohíba el **cifrado** o que obligue a la instalación de **puertas traseras**:

> En octubre de 2014, el entonces director del FBI de los Estados Unidos, James Comey, advirtió que el “**cifrado** amenaza con llevarnos a todos por un mal camino (***going dark***)”, y pidió que se inicie un debate sobre la obligación de las empresas de proporcionar acceso a “**puerta trasera**” en los servicios cifrados. El debate sobre este tema continúa en los Estados Unidos. En 2016, el FBI inició un proceso contra Apple, que recibió y objetó al menos 11 órdenes judiciales, en el que buscaba obligar a la compañía a construir una nueva versión del sistema operativo del iPhone que evadiera las funcionalidades de seguridad para instalarlo en un celular recuperado durante una investigación sobre los ataques terroristas de San Bernardino que ocurrieron a finales de 2015. El FBI finalmente retiró el proceso después de que una “parte externa” ayudara al Gobierno a ingresar al iPhone. En 2019, el Fiscal General William Barr revivió el largo debate sobre el **cifrado** durante una

conferencia de ciberseguridad organizada por el FBI y la Universidad de Fordham. Sus declaraciones volvían a remarcar que las comunicaciones cifradas permitían a los terroristas planear ataques con impunidad y a los criminales actuar libremente. Más recientemente, en 2020, el Congreso de los Estados Unidos está considerando un proyecto de ley para combatir la explotación infantil en línea, conocido como la Ley de Eliminación de la Negligencia Abusiva y Descuidada de las Tecnologías Interactivas (*EARN IT Act*), cuestionada por una coalición de organizaciones de la sociedad civil estadounidense que denuncian que no hay manera posible de hacer lo que el proyecto requiere sin socavar el **cifrado**.

En junio de 2015, el entonces Primer Ministro David Cameron dijo al Parlamento británico que tenía la intención de "asegurar que los terroristas no tengan un espacio seguro para comunicarse". En 2016, se aprobó la Ley de Poderes de Investigación, que amplía las facultades de vigilancia electrónica de la comunidad de inteligencia y la policía en el Reino Unido. La ley ha sido muy polémica por muchos motivos, entre ellos, le exige a los proveedores de telecomunicaciones británicos tener la capacidad de eliminar el **cifrado** que aplican cuando sea factible; sin embargo, las empresas extranjeras no están obligadas a eliminar el **cifrado**.



El entonces Fiscal General de Colombia, Néstor Humberto Martínez, también insinuó en 2017 que las empresas proveedoras de servicio de mensajes de texto y voz cifrado no deberían operar en el país si no permiten el acceso de las autoridades a las comunicaciones en una investigación criminal.

En 2019, los Estados Unidos, el Reino Unido y Australia enviaron una carta a Facebook presionándole para que creara una **puerta trasera** en sus aplicaciones de mensajería cifrada para permita a los gobiernos acceder al contenido de las comunicaciones privadas, con el fin de combatir la explotación y el abuso infantil.

Sin embargo, también hay algunos avances positivos en esta área, ya que el reconocimiento de que el debilitamiento del **cifrado** (una herramienta de ciberseguridad) en nombre de la ciberseguridad, probablemente conduzca a un deterioro de la seguridad, sin mencionar las protecciones a los derechos humanos:

En junio de 2015, el Relator Especial de Naciones Unidas sobre la libertad de opinión y expresión, David Kaye, publicó un informe histórico que señaló que el cifrado y el **anonimato** crean una "zona de privacidad" que es esencial para el disfrute de los derechos a la libertad de opinión y expresión

En septiembre de 2015, el Gobierno de la India presentó una propuesta normativa que habría anulado el **cifrado** al exigir a la ciudadanía almacenara versiones en texto sin formato de sus datos cifrados durante 90 días y que estuviesen disponibles para las agencias de seguridad. La política fue retirada tras la indignación pública que siguió a su publicación.



En enero de 2016, el Gobierno francés rechazó un proyecto de ley que habría requerido a los fabricantes de equipos considerar las necesidades de las autoridades policiales y de inteligencia al diseñar tecnologías, insertando **puertas traseras** en los dispositivos.

En una carta publicada en enero de 2016, el Ministerio holandés de Seguridad y Justicia dijo que cualquier movimiento para debilitar o crear **puertas traseras** al **cifrado** “tendría consecuencias indeseables para la seguridad de la información almacenada y comunicada, y la integridad de los sistemas de TIC, que son cada vez más importantes para el funcionamiento de la sociedad”.

En 2019, Facebook, respondiendo a la carta de los Estados Unidos, el Reino Unido y Australia, mostró su firme oposición a los intentos de los gobiernos de construir **puertas traseras**, reiterando su compromiso por la privacidad y seguridad de todas las personas.

¿NO HEMOS ESTADO AQUÍ ANTES? LAS GUERRAS CRIPTOGRÁFICAS

Los debates sobre la restricción al **cifrado** no son nada nuevo. En la década de los 90, el mundo fue testigo de las primeras “guerras criptográficas” que enfrentaron al Gobierno de los Estados Unidos contra el sector tecnológico. En la década de 70, el Gobierno estadounidense clasificó los algoritmos de **cifrado** como una munición para propósitos de control de las exportaciones, lo que significaba que el **cifrado** desarrollado en los Estados Unidos no podía ser compartido más allá de sus fronteras. En ese momento, los productos de **cifrado** se utilizaban principalmente en el campo militar, más que en el civil.

Avanzamos rápidamente hacia la década de los 90 cuando los productos de cifrado del mercado masivo como *Pretty-Good-Privacy* (PGP) se estaban poniendo a disposición del público, y el Gobierno estadounidense trató de hacer cumplir los controles contra las personas que estaban desarrollando productos de **cifrado**. Fue así como intentaron procesar al desarrollador de PGP, Phil Zimmerman. Un grupo de técnicos y activistas reaccionaron imprimiendo códigos y claves cifradas en camisetas y en copias impresas cuando viajaban al extranjero como protesta contra la aplicación de los controles por parte de los Estados Unidos.

Más o menos al mismo tiempo, el **cifrado** se estaba extendiendo en las redes de telecomunicaciones digitales. En respuesta, la administración Clinton intentó que la industria tecnológica adoptara un esquema de **puertas traseras de cifrado** llamado “*Clipper Chip*”, un dispositivo de cifrado físico que los operadores de redes colocarían en sus redes, del que el Gobierno tendría una clave de descifrado. Cuando la industria rechazó este sistema, el Gobierno de los Estados Unidos presionó a favor de otras formas de **custodia de claves** y alentó a otros países, incluido el Reino Unido, a que propusieran sistemas similares. Sin embargo, la oposición de la industria, incluyendo la bancaria, la indignación de la sociedad civil y un cambio de administración después de las elecciones estadounidenses en el 2000, vieron cómo se abandonaron los intentos de depósito de claves.

Los controles de exportación de la criptografía siguen existiendo en muchos países, pero rara vez se aplican a los productos y servicios comerciales de **cifrado**.

La protección y promoción del **cifrado** es fundamental no solo para garantizar una robusta ciberseguridad, sino también para el disfrute de los derechos humanos en espacios privados donde las opiniones e ideas se puedan compartir libremente. Blindar las comunicaciones contra la interferencia externa es la única manera como las personas usuarias de internet, defensoras de derechos humanos, de oposición política, disidentes y activistas, además de periodistas de investigación, puedan operar de manera segura. También existe un imperativo de derechos humanos en la adopción masiva y no selectiva del **cifrado**. En la actualidad, las personas que usan herramientas cifradas para proteger sus comunicaciones pueden, irónicamente, ser sujetas a un escrutinio adicional por parte del Estado. El uso generalizado del **cifrado** evitaría este fenómeno.

USO DEL ANONIMATO EN INTERNET

El **cifrado** protege contra la interferencia en relación con el contenido de una comunicación, pero no garantiza el **anonimato** de la persona remitente o destinataria de esa comunicación, que requiere tomar medidas adicionales para enmascarar la propia identidad y eludir su detección. Estas medidas pueden ir desde el uso de un seudónimo hasta el uso de tarjetas SIM no registradas o el uso de herramientas de anonimización, como los enrutadores de cebolla (*onion routers*). Dada la naturaleza de las herramientas de análisis de datos, múltiples capas de anonimato pueden ser necesarias para evitar realmente que una persona sea identificada, sobre todo, cuando se usan herramientas y plataformas digitales para comunicarse. Permanecer en el **anonimato** es una forma de ejercer la privacidad, y también puede ser un medio o un precursor para expresarse libremente, especialmente cuando se comunican opiniones, creencias o afiliaciones polémicas que puedan desafiar el *statu quo* y poner a la persona que las expresa en peligro o riesgo de ser víctima de otras violaciones de derechos.

LA DEEP WEB, DARK WEB Y TOR

Con la omnipresente recopilación de datos por empresas y gobiernos, es cada vez más difícil mantener el anonimato en línea. Incluso el uso del cifrado no proporciona anonimato, y es poco probable que el uso de un seudónimo proteja nuestra identidad completamente, especialmente cuando las legislaciones nacionales exigen la retención de datos del uso de internet o servicios móviles, o el registro de tarjetas SIM.

Se suponía que internet nunca iba a ser un espacio gobernado e indexado, pero partes de esta red se han vuelto cada vez más así. Sin embargo, hay otras partes que no están indexadas y organizadas: la "web profunda" (*deep web*) hace referencia a todos los sitios web que los motores de búsqueda no pueden encontrar. Estos incluyen bases de datos, páginas de *webmail* y sitios a los que solo se accede pagando.

En la web profunda existe un conjunto de sitios web que son visibles públicamente, pero que ocultan las direcciones IP de los servidores que los ejecutan. Cualquier persona puede visitarlos, pero no se pueden encontrar en los motores de búsqueda. Y es difícil averiguar quién los ejecuta, porque la identidad de quien controla el sitio suele estar oculta usando la herramienta de cifrado TOR, o servicios similares como I2P. Este conjunto de sitios web a veces se le llama la "web oscura" (*dark web*), con la implicación y presunción de que alberga principalmente actividades ilegales.

Para acceder a un sitio en la *dark web*, las personas necesitan usar la misma herramienta de cifrado que el sitio, normalmente el navegador TOR. Sin embargo, las personas pueden y usan este navegador para actividades normales de navegación; para ocultar su ubicación y uso, y para dificultar que sus actividad en línea sea rastreada hasta ella. TOR es utilizada por personas defensores de derechos humanos, periodistas y activistas de todo el mundo.

El **anonimato** y los derechos que protegen están amenazados por una serie de medidas supuestamente diseñadas para combatir el ciberdelito. Estas medidas incluyen el uso obligatorio o el registro de identidad, incluidas las leyes que exigen que las personas blogueras y comentaristas en internet utilicen sus nombres reales, el registro de tarjetas SIM y direcciones IP, el uso de identificación personal en los cibercafés y la prohibición de redes privadas virtuales (véase en la página 36 una discusión de cómo estas medidas pueden amenazar los derechos humanos).

El *software* de anonimización, en particular el navegador TOR, está especialmente amenazado ahora que las agencias policiales y de inteligencia de todo el mundo intentan superar los obstáculos para vigilar delitos graves y crimen organizado en "web oscura". Aunque en su mayor parte, los debates sobre políticas públicas reconocen el "doble uso" de TOR, que es una herramienta fundamental para las personas defensoras de derechos humanos y periodistas, y que también es donde operan mercados como la ruta de la seda para productos robados e ilícitos, las políticas contra el ciberdelito están cada vez más centradas en cómo infiltrar esta red. En noviembre de 2015, la Agencia de Inteligencia del Reino Unido (GCHQ) y su equivalente en los Estados Unidos, la Agencia de Seguridad Nacional (NSA) anunciaron la conformación de una célula de operaciones conjuntas para combatir la explotación infantil en línea en los servicios ocultos de la red TOR: "[estamos] comprometidos a garantizar que ninguna lugar de internet, incluida la web oscura, pueda ser utilizada con impunidad por los delincuentes para llevar a cabo sus actividades ilegales".

Aunque esta puede ser una misión legítima, las técnicas utilizadas por las agencias de inteligencia en este ámbito pueden, de hecho, tener el impacto de socavar la ciberseguridad. Por ejemplo, estas técnicas incluyen:

El uso de ***malware*** o actividades de explotación de redes informáticas por parte de agencias gubernamentales. Esto se basa en el almacenamiento y manipulación de **vulnerabilidades** –debilidades en el *software* o *hardware*– que de otro modo deberían informarse a los fabricantes de dicho *software* o *hardware* para que puedan repararlas. Mientras los gobiernos se guarden el conocimiento de estas debilidades para usarlas como posibles herramientas ofensivas, los *software* o *hardware* siguen siendo inseguros y pueden sufrir ataques de otros actores. Existe un creciente movimiento a favor de imponer obligaciones a los gobiernos de divulgar en lugar de almacenar la información sobre estas **vulnerabilidades** para así apoyar los objetivos de ciberseguridad.

El uso de actualizaciones de seguridad falsas para instalar ***malware*** en un dispositivo o programa que pueda utilizarse para fines de vigilancia. Esto socava la confianza en las actualizaciones de seguridad y disuade a las personas usuarias de descargarlas.

El apetito de las agencias de inteligencia de obtener herramientas de vigilancia aún más intrusivas continúa creciendo. Los documentos de los archivos de Snowden revelaron cuán lejos han ido las agencias de inteligencia de los Estados Unidos y el Reino Unido para desarrollar *software* de intrusión, empleando ***malware***, buscando utilizar a los administradores del sistema para **hackear** empresas y redes enteras. Por ejemplo, el Reino Unido estableció una Unidad Nacional de Delitos Cibernéticos al interior de la Agencia Nacional del Crimen (NCA), una agencia policial, no de inteligencia. La NCA pretende diseñar su propio *software* de intrusión y lanzar una unidad de reclutamiento para encontrar programadores que diseñen troyanos, un tipo de ***malware*** diseñado para proporcionar acceso remoto no autorizado al dispositivo de una persona. Una filtración de documentos corporativos del fabricante de ***malware***, Hacking Team, en julio de 2015, mostró que países como Azerbaiyán, Kazajstán, Uzbekistán, Rusia, Bahrein, Arabia Saudita y los Emiratos

Árabes Unidos han comprado herramientas de ***hacking*** para usarlas en la recopilación de inteligencia. Autoridades de Brasil, Chile, Colombia, Ecuador, Honduras, México y Panamá también compraron *software* a este fabricante italiano de algunos de los programas de espionaje más invasivos del mundo. De otra parte, aunque en los documentos filtrados no hay información de adquisición de programas, parece que Argentina, Guatemala, Paraguay, Uruguay y Venezuela llegaron a negociar con la compañía.

Las actividades de ***hacking*** parecen exacerbar las inseguridades cibernéticas, en lugar de contribuir a una mayor ciberseguridad por medio de avances en la vigilancia policial y la detección de ciberdelitos. Por ello, hacen falta más controles al respecto.

RESTRICCIONES Y CORTES DE INTERNET

A medida que el acceso gratuito y seguro a internet se convierte cada vez más en un requisito previo para el disfrute de una gama de derechos fundamentales, desde el derecho a la libertad de expresión hasta el de la educación, las restricciones a la funcionalidad de internet pueden tener graves efectos para los derechos humanos. Sin embargo, hay una tendencia creciente, como se muestra a continuación, a que los gobiernos ordenen la limitación, la ralentización o el corte de internet o la prohibición de ciertos sitios o servicios. A menudo, los cortes de internet se justifican por motivos de seguridad nacional y de ciberseguridad, y ocurren en el contexto de acontecimientos políticos, elecciones y manifestaciones.

Las restricciones al funcionamiento y uso de internet en nombre de la ciberseguridad tienen implicaciones de gran alcance para los derechos humanos.

Algunos ejemplos destacados de cortes de internet incluyen:

Durante las elecciones presidenciales y parlamentarias ugandesas de febrero de 2016, la Comisión de Comunicaciones de Uganda ordenó un corte de internet de tres días, y requirió que los proveedores de servicios móviles como MTN Uganda bloquearan el acceso de las personas usuarias a los sitios de redes sociales y las transferencias móviles de dinero.

Durante las protestas de enero de 2011 en la Plaza Tahrir, el Gobierno egipcio ordenó el corte de la internet en Egipto.

A raíz de los ataques terroristas de marzo de 2016 en Ankara, el Gobierno turco impuso un bloqueo total de los medios de comunicación y prohibió que se reportara en “internet y redes sociales”. También impuso una limitación de velocidad a nivel de los proveedores de servicios de internet con el fin negar cualquier acceso a la cobertura del ataque. El Gobierno había emitido previamente una prohibición general del uso de Twitter en el país.

Durante los ataques cibernéticos de Estonia en 2007, el Gobierno tomó medidas para bloquear todo el tráfico web internacional con el fin de detener la ola de **DDoS** o ataques de denegación de servicio a los servidores gubernamentales.

En Latinoamérica también se han registrado prácticas para restringir el flujo de discursos y contenidos multimedia durante protestas. En Venezuela, se han

registrados bloqueos intermitentes de redes sociales, plataformas digitales y medios de comunicación específicos. En Nicaragua, los cortes intermitentes de internet estuvieron presentes durante las protestas de 2018 y 2019 mediante “apagones” completos del internet en regiones específicas del país. En Ecuador, durante las protestas de finales de 2019, servicios como WhatsApp y Twitter presentaron fallas en la descarga de videos e imágenes. También se reportó que los servidores de imágenes y contenido de Facebook y WhatsApp estuvieron inaccesibles a través del operador de telecomunicaciones estatal Corporación Nacional de Telecomunicaciones (CNT).

En agosto de 2019, el Gobierno de la India cortó internet en Cachemira después de revocar su autonomía y condición de estado, al tiempo que instituyó una campaña de represión en el territorio en disputa. El Gobierno justificó el corte total de internet como una medida necesaria para evitar protestas violentas y ataques militantes en esa zona del país, que alberga una prolongada insurgencia contra la India. En enero de 2020, el Gobierno indio restableció parcialmente los servicios de internet.

De acuerdo al informe del Proyecto STOP de la ONG internacional Access Now, en 2019 se registraron al menos 213 cortes de internet alrededor del mundo. India encabeza la lista mundial de países con una cifra de 121 cortes. En segundo lugar, se encuentra Venezuela, que registra 12 bloqueos al acceso a redes sociales en 2019. Le siguen Yemen, Irak, Argelia y Etiopía entre los países con más cortes de internet.

Además del aumento significativo de cortes de internet que se registraron en ese año, se ha identificado que los cortes duran más, afectan a más personas y se dirigen cada vez más contra grupos vulnerables.

Las restricciones al funcionamiento y uso de internet en nombre de la ciberseguridad tienen implicaciones de gran alcance para los derechos humanos. No solo impiden que las personas compartan y accedan a la información, sino que impiden el disfrute de los derechos humanos que dependen de internet, desde la libertad de movimiento y asociación, a la participación política.

INCORPORAR DERECHOS HUMANOS A LA FORMULACIÓN DE POLÍTICAS SOBRE CIBERDELITOS

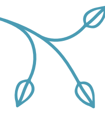
A diferencia del espacio de la política de seguridad de la información, los derechos humanos ya están presentes en el discurso sobre ciberdelitos. Sin embargo, hasta ahora la tendencia es que los derechos humanos reciban solo una mención simbólica, o que se les utilice como una intrusión “en blanco y negro” en otros derechos, por ejemplo, cuando se utilizan los derechos de niñas, niños y adolescentes a estar libres de explotación y abuso para justificar la implementación de sistemas de bloqueo y filtrado.

Estas son algunas recomendaciones para incorporar los derechos humanos a la política de delitos informáticos de una manera que sea significativa y que equilibre adecuadamente consideraciones de derechos humanos cuando estén en conflicto:



Examinar la legislación sobre ciberdelitos y buscar la eliminación de las disposiciones que regulan la difusión en línea de contenido compatible con los derechos humanos.

La legislación propuesta contra los ciberdelitos a menudo evade el escrutinio de las personas defensoras de derechos humanos porque se percibe como demasiado técnica o específica. Sin embargo, existen recursos disponibles para que puedan evaluar la legislación sobre ciberdelitos y analizar si interfiere indebidamente con derechos humanos como el de la privacidad. Por ejemplo, la organización internacional Article 19 ha realizado muchos análisis de legislaciones sobre ciberdelitos desde estos ángulos. El Consejo de Europa también proporciona una guía de derechos humanos para las personas usuarias de internet. Es importante comprender las fuentes utilizadas para redactar proyectos de ley sobre ciberdelitos. Cuando se haya utilizado una “ley modelo”, el análisis de la misma (véase “Recursos seleccionados”) y el conocimiento de sus deficiencias en relación con las mejores prácticas y derecho internacionales pueden ser útiles para la promoción efectiva de los derechos humanos.



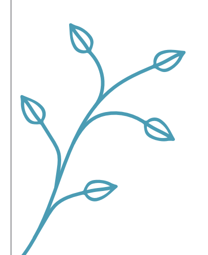


Hacer campaña contra el uso de los “ciberdelitos” como medio para criminalizar el activismo y socavar la libertad de internet.

Las personas defensoras de derechos humanos deben hacer frente a quienes exageran las amenazas de los ciberdelitos, o la importancia de la ciberseguridad, para acabar con el discurso legítimo, el activismo y la expresión en línea.



Hacer campaña para que los gobiernos proporcionen justificaciones basadas en la evidencia para cualquier nuevo poder de vigilancia.



A raíz de las revelaciones de Snowden, ha habido casos judiciales y consultas públicas que han llevado a una mayor transparencia en cuanto a las técnicas de vigilancia, a la desclasificación de sentencias judiciales secretas y al reconocimiento de la existencia de ciertos poderes por parte de los gobiernos que durante mucho tiempo negaron tenerlos. Estos avances demuestran que los gobiernos pueden ser más transparentes sobre sus capacidades de vigilancia sin socavar la efectividad de esas capacidades. Se debe alentar al público a pedir que la policía y las agencias de inteligencia mejoren su rendición de cuentas con respecto a la vigilancia, en lugar de aceptar razonamientos amplios sobre el terrorismo o el ciberdelito como justificaciones para la intrusión en la privacidad.



Abogar contra los programas de vigilancia masiva que faciliten las intrusiones indiscriminadas y generales en los derechos a la privacidad y la libertad de expresión.

La práctica estatal cuando se trata de **vigilancia masiva** está cada vez más alejada de las normas de derechos humanos pronunciadas por los mecanismos regionales e internacionales de derechos humanos. La lucha contra la legitimidad y la legalidad de la vigilancia general e indiscriminada continúa, y las personas defensores de los derechos humanos deben influir: exigir a los gobiernos que la vigilancia se ajuste a las normas de derechos humanos y educar al público sobre las implicaciones de la **vigilancia masiva**.





Hacer campaña para obtener más fondos de investigación y apoyo financiero sostenible a largo plazo para que las personas defensoras de los derechos humanos participen en los debates de ciberseguridad.

Las campañas relacionadas con los recursos asignados a la ciberseguridad también podrían centrarse en la necesidad de financiar auditorías de seguridad críticas para los principales bloques de construcción de *software* libre, como *Linux*, *OpenSSL*, *OpenOffice*, que a menudo crean y mantienen muy pocas personas que con frecuencia trabajan *ad honorem*.



Hacer un llamado a los gobiernos para que se comprometan a apoyar y proteger el cifrado como una herramienta esencial de la ciberseguridad y una condición previa para el disfrute de los derechos humanos.

Las personas defensoras de derechos humanos deben equiparse con las herramientas y argumentos para denunciar las prohibiciones propuestas contra el **cifrado** como ineficaces, contraproducentes y peligrosas para la ciberseguridad. Apoyar a las empresas que crean y publican herramientas y servicios cifrados también puede ser un medio eficaz de apuntalar el apoyo al **cifrado**. Es fundamental que el público también entienda que el **cifrado** es una herramienta para la ciberseguridad y no una herramienta que se oponga a ella.





Hacer campaña contra las restricciones en internet, incluidas aquellas contra el anonimato.

El **anonimato** en línea no se debe ver como una cosa del pasado, o una causa perdida. Es un componente esencial de los derecho a la libertad de expresión y la privacidad, y algo por lo que vale la pena luchar. Se debe educar a las empresas sobre las problemáticas implicaciones de las políticas de uso de nombres reales y alentarlas a permitir que las personas usuarias hagan uso de seudónimos. Las leyes que requieren el registro obligatorio de tarjetas SIM deben ser criticadas tanto por razones de privacidad como por la ineficacia de esta medida para prevenir y detectar delitos.

Las personas defensoras de derechos humanos deben rechazar aquellos esfuerzos de los gobiernos de erradicar el software de anonimización como el navegador TOR, y señalar el papel esencial que desempeña la red TOR para que las propias personas defensoras de derechos humanos puedan comunicarse de manera segura.

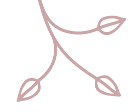




4 LA CIBERSEGURIDAD COMO CIBERCONFLICTO

¿Significa esto la guerra en el ciberespacio?

El aspecto de la formulación de políticas de ciberseguridad que atrae la mayor atención pública es el área en la que las políticas están menos maduras: la cuestión de qué leyes y normas deben regular la forma en la que los gobiernos se relacionan entre sí en el ciberespacio. Para decirlo de manera más simple: ¿cuáles son las reglas que deben cumplir los Estados?



PRINCIPALES PRIORIDADES Y DEBATES DE POLÍTICA PÚBLICA

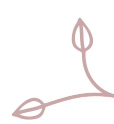
La gente del común (léase, aquellas que no son expertas en derecho internacional) podría sorprenderse al descubrir el alto grado de acuerdo que existe entre los gobiernos sobre las reglas de relaciones internacionales y seguridad: las condiciones bajo las que se justifica el uso de la fuerza de un Estado contra otro, y los términos en que se debe llevar a cabo el conflicto. Estas cuestiones están reguladas por la Carta de las Naciones Unidas y la variedad de tratados y derecho consuetudinario que comprenden el derecho internacional humanitario. Incluso si los gobiernos no siempre cumplen con estas reglas, aún así las reconocen y las respaldan, aunque sea hipócritamente. Cuando se trata de conflictos fuera de internet, es mucho más probable que los Estados justifiquen las flagrantes infracciones a las reglas como excepciones ("las reglas no se aplican aquí porque…"), en lugar de rechazarlas tajantemente ("no hay reglas…").

Desde la aparición de la perspectiva de la "ciberguerra" y sus numerosas variaciones y precursores, como los **ciberataques**, el ciberespionaje, las operaciones y vandalismo cibernético, hay un debate creciente sobre qué reglas, si las hubiera, se aplican al conflicto internacional en el ciberespacio. Los temas sin resolver incluyen:

¿Qué constituye un **ciberataque**?

¿Bajo qué circunstancias puede un Estado tomar medidas para adelantarse a un **ciberataque**?

¿A qué nivel se considera que una ciberoperación constituye un **ciberataque** equivalente al "uso de la fuerza" según la Carta de las Naciones Unidas?



¿Pueden los Estados responder legítimamente a un **ciberataque** con el uso de la fuerza fuera de internet?

¿Deberían los Estados abstenerse de atacar la infraestructura crítica de otros Estados en tiempos de paz? ¿Qué tal durante un conflicto armado real?

¿Qué es un ciberarma y cómo se puede emplear legítimamente?

¿Cuál es la forma apropiada de regular el uso de sistemas de armas autónomas?

Una pregunta general es ¿qué papel juegan el derecho internacional de los derechos humanos con respecto a las normas en el ciberespacio? El Manual de Tallin (ver el recuadro en la página 104), una iniciativa académica de derecho indicativo (*soft law*), aboga por la aplicación del derecho internacional humanitario a las cuestiones del ciberconflicto. La creación del manual fue financiada por la Organización del Tratado del Atlántico Norte (OTAN), aunque no se consultó a los Estados miembros y se llevó a cabo a puerta cerrada, sin oportunidad para que se escucharan las voces de los derechos humanos. Como resultado, el conjunto de leyes y normas que elabora difiere considerablemente de las leyes de derechos humanos y, posiblemente, proporciona un nivel más bajo de protección para las personas.

Por ejemplo, el concepto de proporcionalidad en virtud del derecho internacional humanitario es mucho más maleable que en los derechos humanos. No le preocupa el impacto de una medida particular (como un bombardeo) en el disfrute de los derechos humanos de todas las personas (como los grupos combatientes enemigos), sino solo el daño colateral a civiles. La proporcionalidad bajo los derechos humanos es mucho más exigente.

EL MANUAL DE TALLIN

El Manual de Tallin sobre el Derecho Internacional Aplicable a la Ciberguerra es una iniciativa académica convocada por el Centro de Excelencia Cooperativo de Defensa Cibernética de la OTAN (CCD COE). El manual, elaborado por un grupo de veinte personas expertas internacionales y cuya primera edición fue publicado en abril de 2013, tiene por objeto identificar las normas de la "letra dura" del derecho internacional pertinentes en el contexto cibernético. Esto quiere decir que se centra en el derecho que está escrito en tratados y textos –no en el derecho que se desarrolla a través de la jurisprudencia, la costumbre o la práctica– y proporciona comentarios sobre la aplicación de esas normas.

Si bien el manual original se centraba en las ciberoperaciones más perturbadoras –las que alcanzan el nivel de "ataques armados" cuando se aplica por analogía el derecho internacional vigente sobre la guerra–, la edición de 2017 aborda las ciberoperaciones que no alcanzan ese umbral, y proporciona orientación sobre los regímenes jurídicos aplicables.

La primera edición del Manual de Tallin ha sido objeto de análisis y críticas sustanciales (véase, por ejemplo, *Cyber War Will Not Take Place* de Thomas Rid). A un nivel muy básico, ciertamente, el manual contribuye a la securitización del discurso sobre la ciberseguridad y corre el riesgo de alentar la intensificación de los debates sobre las actividades en el ciberespacio hasta el nivel de un conflicto. Si bien este manual es un trabajo académico, que no fue sometido a un proceso de desarrollo de múltiples partes interesadas y no incluye aportaciones ni comentarios de la sociedad civil, suele ser citado como una fuente autorizada en los procesos de elaboración de políticas relativas a las normas en torno a los ciberconflictos.



En respuesta a las críticas, el grupo internacional de expertos que trabajaron en la segunda versión del manual fue más amplio tanto en su origen (incluyendo miembros de Tailandia, Japón, China y Belarús) como en su contenido (incluyendo personas expertas en derechos humanos, derecho del espacio y derecho internacional de las telecomunicaciones). Incluso se invitó al Comité Internacional de la Cruz Roja (CICR) a que enviara un grupo observador, al igual que a otros Estados y organizaciones.

Tallin 2.0 presenta una gran cantidad de cuestiones jurídicas que suelen plantearse en las ciberoperaciones y examina el estado actual del derecho internacional y la forma en que podría aplicarse a cada situación concreta. En muchos casos, su grupo de redactores no pudo llegar a un consenso, lo que ilustra las complejidades que aún persisten en el mundo cibernético.

En 2017, el Manual se actualizó y extendió a los ciberincidentes más comunes con los que los Estados se encuentran a diario y que están por debajo de los umbrales del uso de la fuerza o el conflicto armado. Tallin 2.0 examina el marco jurídico internacional que se aplica a esas ciberoperaciones. Algunos se refieren al derecho de la responsabilidad del Estado, el derecho del mar, el derecho internacional de las telecomunicaciones, el derecho del espacio, el derecho diplomático y consular, y con respecto a las personas, a la legislación de los derechos humanos al derecho de los derechos humanos. En Tallin 2.0 también se analiza cómo se aplican en el contexto cibernético los principios generales del derecho internacional, como la soberanía, la jurisdicción, la diligencia debida y la prohibición de la intervención.

Al igual que su versión original, Tallin 2.0 representará solo las opiniones de un grupo internacional de personas expertas, pero no de la OTAN ni sus Estados miembros.

Existe el riesgo de que si el debate en torno a las normas aplicables al ciberconflicto excluye las voces de las personas expertas

y defensoras de derechos humanos, y se centra principalmente en el marco relativamente laxo del derecho internacional humanitario, los derechos humanos se verán seriamente en desventaja.

Hay algo de defensa de los derechos humanos en este espacio. Por ejemplo, en 2015, un grupo de organizaciones, incluyendo Artículo 36, el Comité Internacional para el Control de Armas Robóticas y la Coalición *Just Net* (JNC), presentó una declaración ante el Primer Comité sobre Desarme y Seguridad Humana de la Asamblea General de las Naciones Unidas, instando a que las normas sobre ciberconflictos reflejen las siguientes pautas:

> La aplicación del marco jurídico existente, incluida la legislación de los derechos humanos, al ciberespacio. Al mismo tiempo, no debe considerarse suficiente, y los Estados deberán ir más allá de una reiteración de las reglas generales existentes, reconociendo que el ciberespacio debe abordarse en sus propios términos. Internet debe seguir siendo una infraestructura civil y no debe convertirse en el blanco de ataque o en su medio.
>
> El establecimiento por parte de los Estados de las normas más estrictas contra tales ataques, y no desviarse hacia una aceptación o legitimación de la práctica establecida.
>
> El desarrollo de normas que promuevan una internet que se utilice con fines pacíficos y que resista la tendencia actual a normalizar las capacidades ofensivas.

En algunos aspectos, tales directrices son polémicas, ya que pueden alimentar la narrativa del excepcionalismo del ciberespacio que, según algunos, contribuye a dejar de lado las consideraciones tradicionales de derechos humanos.

A diferencia de las dos áreas de ciberpolítica que se elaboran aquí, muchas de las discusiones sobre estas normas siguen ocurriendo de manera bilateral, y hay pocos foros políticos donde se hable formalmente de los ciberconflictos. A continuación presentamos un corto resumen.

FOROS DE POLÍTICA PERTINENTES

Asamblea General de la ONU

La Primera Comisión de la Asamblea General, que se centra en el desarme y la seguridad internacional, ha estado considerando cuestiones de ciberconflicto desde que Rusia presentó un proyecto de resolución en 1998.

En 2004, el Comité convocó a su primer Grupo de Expertos Gubernamentales (GGE) para examinar las amenazas planteadas por la “ciberesfera” y las posibles medidas de cooperación para hacerles frente. Desde entonces, se han establecido seis grupos de trabajo, incluido el GGE 2019-2021. El GGE ha producido tres informes de consenso en 2010, 2013 y 2015; en 2017, el grupo no pudo llegar a ningún resultado consensuado. Si bien los Estados han podido ponerse de acuerdo sobre diversas normas de comportamiento general en el ciberespacio, el derecho internacional solo ha experimentado una evolución tímida: ningún Estado ha negado la aplicabilidad del derecho internacional en el ciberespacio, pero no están de acuerdo sobre la forma en que se aplica el derecho internacional.

En el primer grupo convocado surgieron dos desacuerdos sustanciales: primero, el grado en que el informe debe destacar el impacto de los problemas cibernéticos para la seguridad nacional y los asuntos militares; y segundo, si el tema de la seguridad de la información se relaciona solo con la infraestructura de la información, o se extiende a las inseguridades causadas por el contenido de la información en sí.

Aunque el GGE de 2010 emitió un informe exitoso que alcanzó un consenso sobre la necesidad de un diálogo entre los Estados acerca

de las normas en el ciberespacio y la necesidad de proteger la infraestructura crítica, entre otras cosas, en 2011 surgió nuevamente la cuestión de las inseguridades causadas por el contenido de la información. Ese año, China, Rusia, Tayikistán y Uzbekistán propusieron un proyecto de resolución sobre un código de conducta internacional para la seguridad de la información y solicitaron deliberaciones internacionales al respecto en el marco de la ONU. El proyecto de resolución adoptó una definición de “seguridad de la información” que supera en su alcance la definición técnica más restringida que se analiza en esta guía (consulte la página 43) al hacer referencia a la capacidad de la información misma para causar inseguridad.

En el informe del GGE de 2013 se llegó a un acuerdo sobre una serie de cuestiones sustantivas relacionadas con el desarrollo de normas y, sobre todo, por primera vez, se acordó que el derecho internacional existente se aplica al ciberespacio. El informe afirmó que:

> El derecho internacional, en particular la Carta de las Naciones Unidas, se aplica a la “ciberesfera” y es esencial para un entorno de TIC abierto, seguro, pacífico y accesible.
>
> La soberanía estatal se aplica a la conducta de los Estados en actividades relacionadas con las TIC y a su jurisdicción sobre la infraestructura de las TIC al interior de su territorio.
>
> Los esfuerzos estatales para abordar la seguridad de las TIC deben ir de la mano del respeto por los derechos humanos y las libertades fundamentales. Los Estados no deben usar terceros para cometer actos internacionalmente ilícitos y deben garantizar que sus territorios no sean utilizados por actores no estatales para el uso ilegal de las TIC.
>
> La ONU debe desempeñar un papel importante en la promoción del diálogo entre los Estados miembros.

Estos hallazgos se profundizaron, sin alteraciones sustanciales, en el informe de 2015. También se recomendó, por ejemplo, que los Estados no deben realizar ciberactividades “que dañen intencionalmente la infraestructura crítica o de otra manera perjudiquen el uso y funcionamiento de la infraestructura crítica para brindar servicios al público”. Añadió que, además, no debe respaldar a sabiendas cualquier actividad que dañe los sistemas de información de los equipos de respuesta de emergencia autorizados (como **CERT**) o usar a los **CERT** para participar en actividades internacionales maliciosas.

Quedan preguntas sobre el significado del acuerdo del GGE y las cuestiones no resueltas que no se abordaron en el informe, a saber: ¿cómo se aplica el derecho internacional al ciberespacio? El que no se hubiera llegado a un acuerdo sobre estas cuestiones más sustantivas sugiere que la creación de normas todavía está plagada de las posiciones divergentes de los principales Estados que participan en ella.

En 2017, el GGE no pudo llegar a un consenso, y no pudo entregar un informe final. Los 20 Estados participantes en ese entonces, que representaban el 10% de los miembros de la ONU, no pudieron encontrar un terreno común sobre los derechos de los Estados a responder a los actos internacionalmente ilícitos cometidos mediante el uso de las tecnologías y la aplicabilidad del derecho internacional humanitario en el ciberespacio. El resultado negativo generó una desilusión general sobre el futuro desarrollo de las cibernormas.

A pesar del ambiente de pesimismo, en 2018 la Primera Comisión de la Asamblea General de la ONU reactivó el proceso de negociación sobre cibernormas creando dos nuevos grupo de trabajo sobre la seguridad internacional y el ciberespacio: el GGE 2019-2021 y el Grupo de Trabajo de Composición Abierta (OEWG). El nuevo proceso creado a través del OEWG tiene como tarea continuar desarrollando las reglas, normas y principios de comportamiento responsable de los Estados, discutir las formas de su aplicación y estudiar la posibilidad de establecer un diálogo institucional regular con amplia participación bajo el auspicio de la ONU. En específico, el grupo tiene en su agenda debatir y llegar a consensos sobre la identificación de amenazas existentes y potenciales; la aplicabilidad del derecho internacional; la identificación y/o posible desarrollo de reglas, normas y principios;

la promoción de un diálogo institucional regular; la identificación de medidas de fomento de la confianza; y la creación de capacidad.

Distinto al GGE, su composición es abierta, permitiendo la participación de todos los Estados miembros y celebrando reuniones consultivas con las diferentes partes interesadas: empresas, organizaciones no gubernamentales y el mundo académico. Aunque hasta ahora la participación de actores no gubernamentales ha presentado dificultades, los métodos de trabajo permiten el intercambio de información y conocimiento entre las diferentes partes interesadas.

Darle legitimidad a las cibernormas finalmente requerirá de la aceptación del conjunto de los Estados miembros de la ONU a un nivel más allá de la mera retórica que, a su vez, incluya aportes adicionales de expertos técnicos y de la sociedad civil.

Proceso de Londres y Conferencia Mundial sobre el Ciberspacio (GCCS)

El GCCS se inauguró en 2011 cuando el Reino Unido y los Países Bajos convocaron una reunión de alto nivel sobre ciberseguridad, los ciberdelitos y las normas aplicables al ciberespacio en Londres. Desde entonces, el GCCS se ha reunido en Budapest (2012), Seúl (2013), La Haya (2015) y Nueva Delhi (2017). Su objetivo es proporcionar un entorno de múltiples partes interesadas para deliberar sobre la ciberseguridad y las normas sobre los ciberconflictos, y la transferencia de capacidades en temas de ciberseguridad.

Comité de Lucha contra el Terrorismo del Consejo de Seguridad de la ONU (CTC)

El CTC tiene la responsabilidad de supervisar el cumplimiento de la Resolución 1373 (2001), aprobada después de los ataques terroristas de septiembre de 2001, así como las resoluciones 1624 (2005) y 2178 (2014) que requieren que los Estados penalicen, procesen e investiguen actividades terroristas, la financiación de actividades terroristas, y los combatientes terroristas extranjeros.

Aunque el CTC no tiene un mandato directo para abordar cuestiones de ciberseguridad y ciberconflicto, ha comenzado a examinar los problemas de ciberdelito y ciberseguridad en relación con el uso de internet y las redes sociales por parte de terroristas. En particular, el CTC tiene la intención de continuar evaluando la implementación por parte de los Estados de las resoluciones mencionadas anteriormente, en particular cuando se aplican a internet y las tecnologías digitales, centrándose en fortalecer la cooperación para prevenir el uso de las TIC con fines terroristas y tomando medidas contra la incitación a la violencia en línea. Además, el CTC está trabajando con el sector privado en encontrar respuestas sobre el uso de internet y las TIC con fines terroristas.

Freedom Online Coalition

Establecida en 2011, la *Freedom Online Coalition* está compuesta por 31 Estados miembros (a marzo de 2020) de América, Asia, África, Europa y Medio Oriente, que se han comprometido con el principio de que los derechos humanos se aplican dentro y fuera de internet. La Coalición coordina los esfuerzos diplomáticos relativos a internet y proporciona una plataforma de participación de múltiples partes interesadas, incluso a través de la conferencia anual *Online Freedom*.

La Coalición también ha respaldado un conjunto de recomendaciones para la elaboración de políticas de ciberseguridad que respeten los derechos humanos, así como una definición de ciberseguridad.

Iniciativa de Cooperación Global en el Ciberespacio

Fundada y operada por el EastWest Institute, la Iniciativa es una organización independiente sin fines de lucro que tiene como objetivo crear un espacio de múltiples partes interesadas para reunir a actores dispares para resolver problemas relacionados con la cooperación y el conflicto en el ciberespacio. La Iniciativa convoca cumbres, produce documentos de trabajo y, lo que es más importante, reúne a actores que de otra manera no estarían necesariamente en la misma mesa para discutir el desarrollo de normas en este espacio.



INCORPORAR DERECHOS HUMANOS A LA FORMULACIÓN DE POLITÍCAS SOBRE CIBERCONFLICTOS

La formulación de políticas para el ciberconflicto es el área menos desarrollada de la formulación de políticas de ciberseguridad y se lleva a cabo en gran medida en foros multilaterales que tradicionalmente no están muy abiertos a la sociedad civil. Sin embargo, estas son algunas recomendaciones sobre las formas en que la sociedad civil puede abogar con los Estados para poner los derechos humanos sobre la mesa:



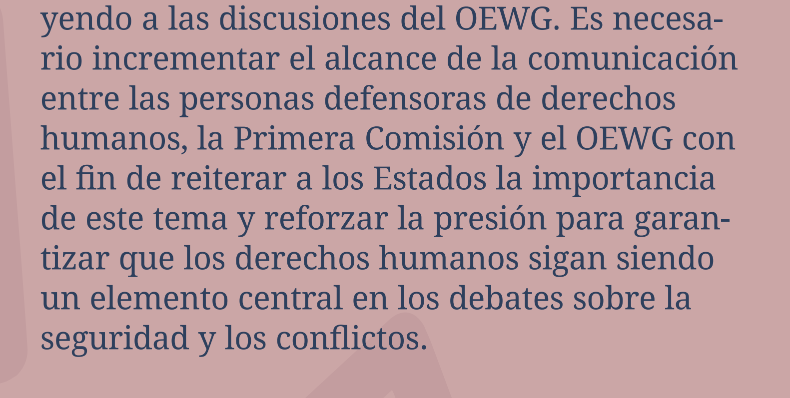
Abogar con los Estados miembros del GGE para asegurar que las consideraciones de derechos humanos sean prioritarias en la agenda del GGE.

El GGE continúa siendo uno de los principales foros en los que se debaten abiertamente las normas sobre los ciberconflicto. Se debe usar el activismo y la educación para que los miembros del GGE sean conscientes de las implicaciones de su trabajo para los derechos humanos.



Trabajar con la Primera Comisión de Desarme en las sesiones anuales de la Asamblea General, en especial en el OWEG.

Las organizaciones de derechos humanos ya están participando en la Primera Comisión al presentar una declaración sobre temas cibernéticos cada año durante el período de sesiones de la Asamblea General y contribuyendo a las discusiones del OEWG. Es necesario incrementar el alcance de la comunicación entre las personas defensoras de derechos humanos, la Primera Comisión y el OEWG con el fin de reiterar a los Estados la importancia de este tema y reforzar la presión para garantizar que los derechos humanos sigan siendo un elemento central en los debates sobre la seguridad y los conflictos.





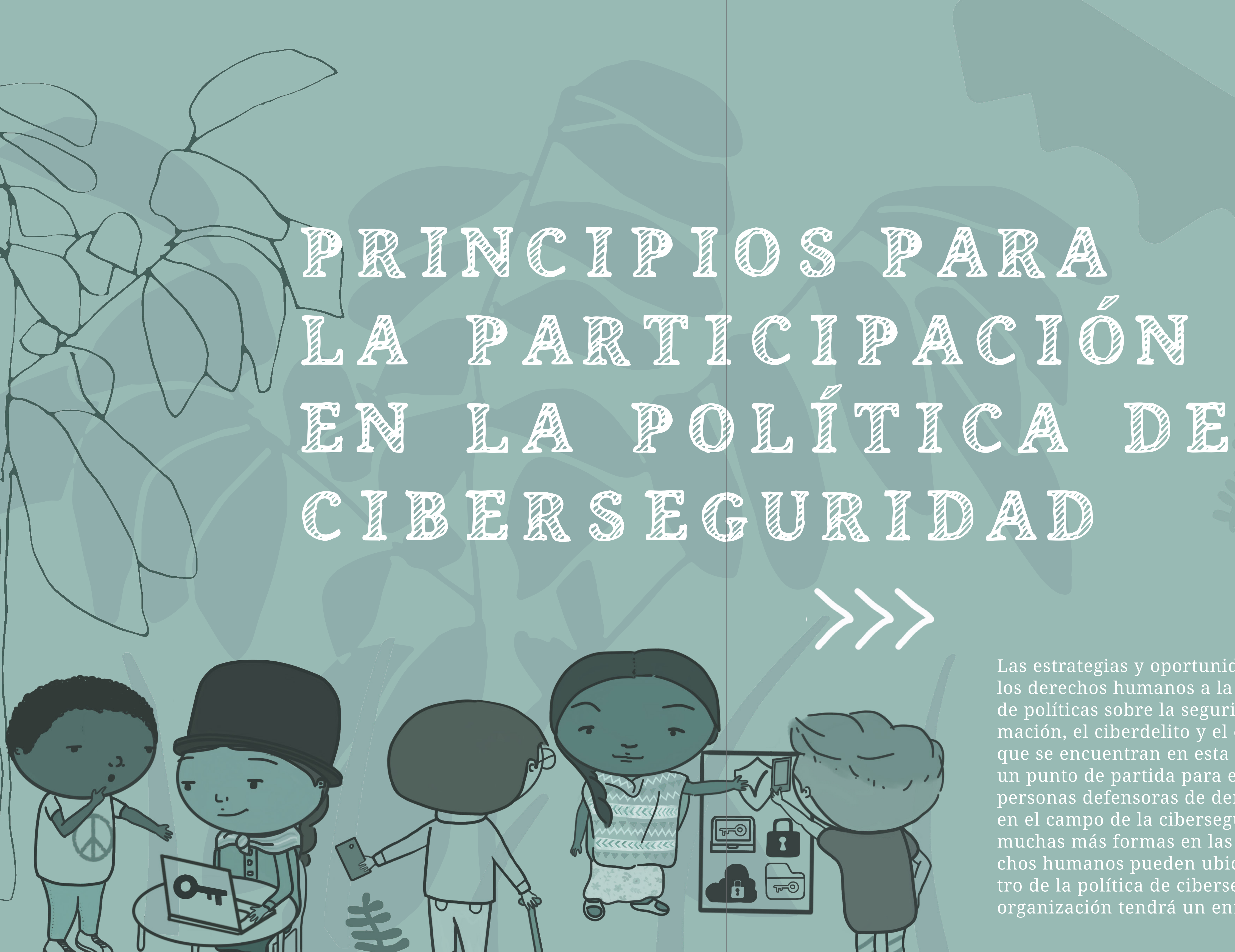
3

Participar en procesos de múltiples partes interesadas, y promover el uso de lenguaje y normas de derechos humanos en todos los debates sobre ciberconflicto.

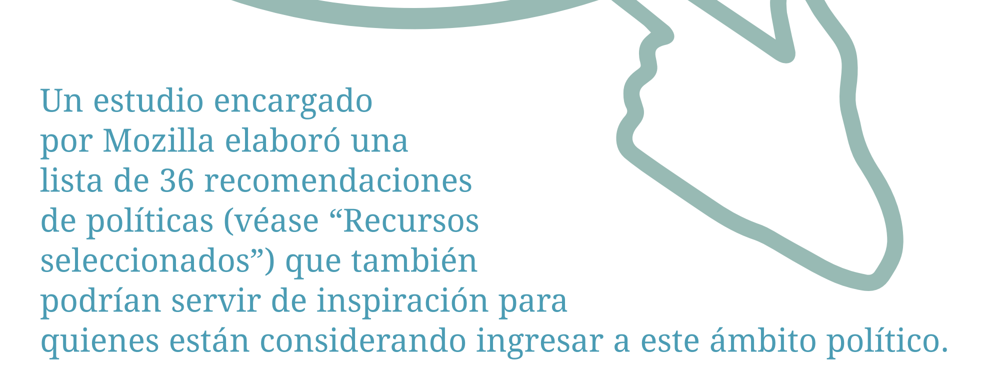
Es fundamental que la sociedad civil esté presente cuando se tomen decisiones sobre las normas del ciberespacio. El solo hecho de asistir a eventos de múltiples partes interesadas como el GCCS (consulte la página 110) demuestra a los Estados y al sector privado que estos temas son de importancia crítica para las personas defensoras de derechos humanos, y garantiza que los derechos humanos permanezcan en la agenda. Igualmente, la publicación de cualquier nueva edición del Manual de Tallin y otras iniciativas académicas y de derecho indicativo deben recibir la debida atención y, cuando se justifique, las críticas de la sociedad civil, para garantizar que las normas propuestas no se acepten o arraiguen sin un debate riguroso.



PRINCIPIOS PARA LA PARTICIPACIÓN EN LA POLÍTICA DE CIBERSEGURIDAD



Las estrategias y oportunidades para llevar los derechos humanos a la formulación de políticas sobre la seguridad de la información, el ciberdelito y el ciberconflicto que se encuentran en esta guía son solo un punto de partida para el trabajo de las personas defensoras de derechos humanos en el campo de la ciberseguridad. Hay muchas más formas en las que los derechos humanos pueden ubicarse en el centro de la política de ciberseguridad, y cada organización tendrá un enfoque diferente.



Un estudio encargado por Mozilla elaboró una lista de 36 recomendaciones de políticas (véase “Recursos seleccionados”) que también podrían servir de inspiración para quienes están considerando ingresar a este ámbito político.



A manera de conclusión, esta sección describe algunos principios de mejores prácticas para el trabajo en políticas de ciberseguridad que las personas defensoras de derechos humanos deberían intentar adoptar e integrar en su trabajo.





1 Tomar control del lenguaje

Como se ha reiterado constantemente a lo largo de esta guía, el lenguaje de la ciberseguridad, a menudo, se utiliza para militarizar o centrar en la seguridad un debate que, de lo contrario, puede enmarcarse en términos de derechos humanos y responsabilidades. El control del lenguaje utilizado puede tener un impacto sobre la dirección que tome la discusión de políticas públicas. Es fundamental que las personas defensoras de derechos humanos enfaticen en todo momento que los problemas de ciberseguridad son problemas de derechos humanos, sin importar desde qué ángulo se los vea.



2 Cambiar el discurso del sacrificio necesario por el refuerzo de derechos

Con demasiada frecuencia, los debates sobre ciberpolítica suponen que la seguridad y los derechos humanos son un juego de suma cero; que para ganar uno, tenemos que renunciar al otro. Las personas defensoras de derechos humanos pueden desempeñar un papel fundamental en la educación de las personas hacedoras de políticas y otros actores sobre cómo los derechos humanos y la ciberseguridad son interdependientes y se refuerzan entre sí, y demostrar cómo la seguridad puede coexistir con el disfrute de los derechos a la privacidad y la libertad de expresión, entre otros.



3 Responder a opiniones con hechos

Participar de manera creíble en los espacios de desarrollo de ciberpolíticas requiere una inversión en la creación de capacidades individuales y organizativas, conocimiento y experiencia en los aspectos técnicos y jurídicos de los que depende el espacio de políticas de ciberseguridad. Las personas defensoras de derechos humanos deben sentirse cómodas con los temas técnicos y áreas emergentes del derecho para garantizar que se les otorgue un lugar igual en la mesa de formulación de políticas.



Apoyar y participar en las iniciativas de múltiples partes interesadas

La realidad de la ciberseguridad, y las amenazas y oportunidades que conlleva, exigen la participación de actores provenientes de una amplia gama de sectores y disciplinas. Este no es un problema que pueda o deba resolverse solo a través del proceso estatal de formulación de políticas; el sector privado, las comunidades técnicas y académicas, y la sociedad civil desempeñan un papel fundamental en el diseño, validación e implementación de políticas de ciberseguridad.

La participación de actores no estatales en el proceso de formulación de políticas puede ayudar a evitar que los discursos se vean dominados por los intereses gubernamentales, y puede disminuir la probabilidad de que se ignoren las cuestiones de derechos humanos.



Utilizar las normas existentes del derecho indicativo para reforzar los mensajes

Las personas defensoras de derechos humanos tienen a su alcance una serie de herramientas claves de defensa y promoción, que incluyen estándares de derecho indicativo tales como los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones (los Principios de Necesidad y Proporcionalidad) y los Principios Globales sobre la Seguridad Nacional y el Derecho a la Información (los Principios de Tshwane). Ambos son instrumentos de derechos humanos que gozan del apoyo de una gran variedad de organizaciones y expertos de la sociedad civil, y proporcionan orientación sobre cómo se deben aplicar los derechos humanos a temas relacionados con tecnología e internet.





Predicar con el ejemplo

Utilizar las herramientas técnicas disponibles para mejorar la ciberseguridad, incluidas las herramientas de **cifrado** y anonimización, y *software* de código abierto es cada vez más importante. Esto puede incentivar a quienes construyen estas herramientas a seguir invirtiendo en ellas y también obtener la aceptación de los gobiernos y del público para su uso.



GLOSARIO

anonimato

La condición de evitar ser identificado. El cifrado no proporciona anonimato. Las herramientas de cifrado aseguran que el contenido de una comunicación sea indescifrable salvo para la persona destinataria, pero no proporcionan anonimato ni a la persona destinataria ni a la remitente. Cuando las partes utilizan herramientas de cifrado, los metadatos asociados a una comunicación (ej. dirección IP) no están cifrados. Si una persona desea permanecer en el anonimato, debe utilizar herramientas y métodos de anonimización, como el uso de seudónimos para una registro o herramientas de anonimización como el navegador TOR.

ataque DDoS

un ataque distribuido de denegación de servicio (DDoS) ocurre cuando varios sistemas informáticos inundan el ancho de banda o los recursos de un sistema específico. Tal ataque es a menudo el resultado de múltiples sistemas comprometidos (por ejemplo, una red de bots) inundando el sistema de destino con su tráfico.

CERT

es la sigla en inglés para Equipo de Respuesta a Emergencias Informáticas. La mayoría de los países mantienen un CERT nacional responsable de responder a los incidentes de ciberseguridad nacional y de apoyar a las empresas que mantienen infraestructura crítica para responder a los incidentes de ciberseguridad.

ciberataque

un término generalmente utilizado para describir el uso de un sistema informático (computadores, teléfonos, etc.) para obtener acceso no autorizado, causar daño o destruir información, dispositivos, sistemas o redes.



cifrado

un proceso matemático de conversión de mensajes, información o datos a un formato que resulte ilegible salvo para las personas remitente y destinataria. El cifrado suele involucrar una clave secreta. La mayoría usamos uno de los tres tipos diferentes de cifrado en nuestro uso cotidiano de internet:

cifrado de extremo a extremo es cuando solo la parte remitente y la destinataria de la comunicación poseen las claves secretas para descifrar sus comunicaciones. Cuando se implementa el cifrado de extremo a extremo, cualquier dispositivo intermedio o proveedor de servicios con acceso a sus comunicaciones electrónicas, o cualquier entidad que intente interceptar las comunicaciones, será incapaz de leer su contenido. Por ejemplo, cualquier persona que intercepte mensajes de iMessages o WhatsApp cifrados de extremo a extremo no podrá leerlos, tampoco las empresas proveedoras de servicio y acceso a internet.

cifrado de disco o dispositivo es el proceso por el que toda la información almacenada en computadores o teléfonos inteligentes está cifrada cuando se encuentra almacenada en el dispositivo. Con el cifrado de dispositivos, los datos ahí almacenados no podrán ser leídos ni accedidos por ninguna persona que no tenga el PIN o la contraseña del dispositivo, incluida la empresa que fabricó el dispositivo o su *software*.

cifrado de transporte es la práctica de cifrar información y datos mientras atraviesan una red informática. Un caso usual del cifrado de transporte es el protocolo HTTPS. Es el "hermano seguro" del protocolo HTTP, que se genera mediante su inclusión dentro de un canal que usa el protocolo *Secure Socket Layer* (SSL) o el más reciente *Transport Layer Security* (TLS). Estos tipos de cifrado, en la práctica, cifran las interacciones de las personas con sitios web específicos a los que se accede a través de sus navegadores web o de una aplicación de teléfono inteligente. Cuando un operador de un sitio web tiene los datos, están en un formato no cifrado. Esto significa que solo se pueden divulgar a la policía o se pueden acceder a ellos de forma inteligible una vez que lleguen a la empresa o al sitio web de destino.

cookies

son pequeños archivos que se almacenan en un computador, más específicamente en el navegador web, de una persona cuando navega en internet. El propósito de las *cookies* es ayudar al sitio web a mantener un registro de las visitas, actividades y registros (*login*) de las personas que navegan en internet. Esto permite personalizar la experiencia de navegación de las personas de acuerdo a los sitios y actividades que realizan en línea.

CSIRT

es la sigla en inglés para Equipo de Respuesta a Incidentes de Seguridad Informática, un término que es intercambiable con CERT (véase más arriba).

custodia de claves

un acuerdo en el que las claves necesarias para descifrar datos cifrados se mantienen en custodia para que, bajo ciertas circunstancias, un tercero autorizado pueda acceder a esas claves y, posteriormente, a los datos que protegen.

going dark

una frase utilizada por la policía estadounidense (y ahora empleada por otros) para describir la disminución de las capacidades de las agencias policiales para acceder al contenido de las comunicaciones debido al mayor uso del cifrado en las tecnologías y servicios cotidianos. Es importante tener en cuenta que, en general, el cifrado no impedirá la interceptación de las comunicaciones ni que las comunicaciones queden totalmente vacías de cualquier información de inteligencia. Las autoridades que practican la interceptación aún podrán obtener cierta información (ej. fecha, hora, remitentes, tamaño, nombre de los sitios webs consultados, etc.) de la comunicación cifrada interceptada.

grooming

es un término para describir la forma en que algunas personas adultas se acercan a niñas, niños y adolescentes para ganar su confianza, crear lazos emocionales y cometer delitos contra su integridad sexual.

hack o hacking (ofensivo)
acceso no autorizado a una aplicación, sistema o red. También conocido como explotación de una red informática, intrusión, interferencia de equipos, acceso remoto y búsqueda remota.

hacktivismo
es el uso de técnicas informáticas como la ciberpiratería como forma de desobediencia civil para promover un programa político o un cambio social. Con raíces en la cultura y ética de los hackers, sus fines suelen estar relacionados con la libertad de expresión, los derechos humanos o los movimientos por la libertad de información. El hacktivismo es a veces ambiguo y existe un desacuerdo significativo sobre el tipo de actividades y propósitos que abarca. Algunas definiciones incluyen actos de ciberterrorismo, mientras que otras simplemente reafirman el uso de la ciberpiratería como actos para alcanzar cambios sociales.

malware
software malicioso que va en contra de las intenciones de la persona usuaria de un dispositivo (ej. computador, teléfono inteligente, tableta), a menudo para proporcionar acceso remoto y divulgar información a personas participantes no autorizadas. El *malware* con frecuencia es encubierto y está disfrazado como otra cosa (una característica que le otorga el nombre de "troyano"), además de que está diseñado para evitar su detección y análisis. El *malware* a menudo permite que un atacante controle ciertas funciones del dispositivo o aplicación, como encender el micrófono o la cámara web de forma remota.

metadatos
se refiere a toda la información que se genera mediante el uso de tecnología de comunicación que no sea el contenido de la comunicación. Si bien la información no necesariamente contiene detalles personales o de su contenido, contiene información sobre los dispositivos que se utilizan, las personas usuarios de los dispositivos y la forma en que se utilizan. Ciertos metadatos, como la dirección IP o números de *cookies*, pueden permitir una identificación indirecta de la persona.

phishing
es una técnica de ingeniería social (manipulación psicológica de personas para realizar acciones o divulgar información confidencial) que se utiliza para engañar a las personas con el fin de obtener información sensible como nombres de usuario, contraseñas y detalles de tarjetas de crédito. Típicamente la persona víctima de *phishing* suele ser atraída por comunicaciones que pretenden venir de un remitente de confianza (ej. entidad gubernamental, institución bancaria, etc.)

puertas traseras

un término coloquial que se usa para referirse a las medidas que debilitan o socavan herramientas, dispositivos y servicios de autenticación o de cifrados y que facilita el acceso no autorizado a la información y comunicaciones por parte de actores que no sean los creadores ni hacen parte de la información o las comunicaciones. Hay muchas formas de crear puertas traseras en un sistema o dispositivo. En el caso del cifrado, estas pueden incluir medidas estatales que obliguen a los proveedores y arquitectos de herramientas y servicios de cifrado a:

* generar y retener claves de cifrado para atender la eventualidad de que se requiera acceso gubernamental a la información y las comunicaciones;

* mantener claves de cifrado en custodia para que, bajo ciertas circunstancias, un tercero autorizado pueda obtener acceso a esas claves para realizar el descifrado (conocido como custodia de claves);

* disminuir la fortaleza del cifrado utilizado en herramientas, dispositivos y servicios cifrados; o

* implementar solo formas aprobadas de cifrado o generadores de números aleatorios específicos aprobados por el Estado y que tengan una debilidad conocida.

Otra forma de puerta trasera son las medidas para obligar a las empresas a generar e implementar actualizaciones de *software* que podrían disminuir o eliminar el cifrado de un dispositivo, herramienta o servicio en particular. También se puede hablar de puertas traseras cuando se infecta un dispositivo o un sistema con un programa malicioso que va a abrir un acceso remoto no autorizado, lo que generalmente se denomina *hacking*, la explotación de una red informática o interferencia de equipos.

ransomware

un tipo de *malware* que restringe el acceso al computador o dispositivo infectado de alguna manera, y exige que la persona pague un rescate a los operadores del *malware* para levantar la restricción.

red de bots

un grupo de computadores conectados a internet que, aunque sus propietarios no lo sepan, se han configurado para reenviar transmisiones y/o generar ataques (incluso *spam* o virus) hacia otros computadores en internet.

tratados de asistencia legal recíproca o MLAT

es un acuerdo entre dos o más países con el propósito de reunir e intercambiar información en un esfuerzo por hacer cumplir leyes penales.

vigilancia masiva

un término utilizado para describir la vigilancia general e indiscriminada de las personas o su información privada, sin sospecha de ningún delito o intento de señalar a ciertas personas o datos en particular. En los últimos años, se ha utilizado junto con la "interceptación generalizada" del contenido de las comunicaciones y sus metadatos.

vulnerabilidades

fallas de seguridad o defectos en el *software* y *hardware* que son identificados y corregidos ("parchados") periódicamente por quienes diseñan y fabrican.

vulnerabilidades de día cero

cuando una vulnerabilidad no se revela a quien desarrolló el *software*, por lo tanto, puede ser utilizada por actores ofensivos porque no se ha corregido. Las vulnerabilidades de día cero a menudo pueden ser explotadas inmediatamente.



RECURSOS SELECCIONADOS



Access Now. (2019). *Targeted, Cut Off, and Left in the Dark*. The *#KeepItOn Report on Internet Shutdowns* in 2019. Disponible en https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf.

Asociación por los Derechos Civiles. (2018). *La Convención de Cibercrímen de Budapest* y *América Latina: breve guía acerca de su impacto en los derechos y garantías de las personas*. Disponible en https://adc.org.ar/wp-content/uploads/2019/06/035-la-convencion-de-cibercrimen-de-budapest-y-america-latina-vol-1-03-2018.pdf.

Berkman Centre for Internet and Society. (2016). *Don't Panic. Making Progress on the Going Dark Debate*. Disponible en https://dash.harvard.edu/bitstream/handle/1/28552576/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf?sequence=1&isAllowed=y.

Brown, D. y Pytlak, A. (2020). *Why Gender Matters in International Cyber Security*. Disponible en https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf.

Castañeda, J.D. (2016). ¿Es legítima la retención de datos en Colombia? Análisis de una herramienta de vigilancia masiva que restringe los derechos humanos. Disponible en https://web.karisma.org.co/wp-content/uploads/download-manager-files/1454009399wpdm_RETENCION%20DE%20DATOS%20-espanol-.pdf.

Centre for the Democratic Control of the Armed Forces. (2010). *Democratic Governance Challenges of Cyber Security*. Disponible en https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf.

Farrell, H. (2015). *Promoting Norms for Cyberspace*. Council on Foreign Relations. Disponible en https://www.cfr.org/report/promoting-norms-cyberspace.

Freedom Online Coalition. (2015). *Mapping Cybersecurity: A visual overview of relevant global spaces in 2015*. Disponible en https://www.gp-digital.org/wp-content/uploads/2015/07/Mapping-Cybersecurity-----A-Visual-Overview-Of-Relevant-Global-Spaces-In-2015.pdf.

Green, N. y Rossini, C. (2015). *Cyber Security and Human Rights. Public Knowledge*. Disponible en https://www.gp-digital.org/wp-content/uploads/2015/06/GCCS2015-Webinar-Series-Introductory-Text.pdf.

Hawtin, D. y Kovacs, A. (2012) *Cyber Security, Cyber Surveillance and Online Human Rights*. Disponible en https://www.gp-digital.org/wp-content/uploads/pubs/Cyber-Security-Cyber-Surveillance-and-Online-Human-Rights-Kovacs-Hawtin.pdf.

Jamil, Z. (2014). *Cybercrime Model Laws*. Disponible en https://rm.coe.int/090000168048c351.

Jardine, E. (2015). *The Dark Web Dilemma: Tor, Anonymity and Online Policing*. Global Paper Series 21: Commission on Internet Governance. Disponible en https://www.cigionline.org/sites/default/files/no.21.pdf.

Mozilla. (2015). *Mozilla Cybersecurity Delphi 1.0: Towards a User-centric Policy Framework*. Disponible en https://blog.mozilla.org/netpolicy/files/2015/07/Mozilla-Cybersecurity-Delphi-1.0.pdf.

National Institute for Standards and Technology. (2015). *Interagency Report on Strategic US Government Engagement in International Standardization to Achieve US Objectives for Cybersecurity*. Disponible en http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v1.pdf.

Osula, A.M. (2015). *Accessing Extraterritorially Located Data: Options for States*. NATO *Cooperative Cyber Defence Centre of Excellence*. Disponible en https://ccdcoe.org/uploads/2018/10/Accessing-extraterritorially-located-data-options-for-States_Anna-Maria_Osula.pdf.

Pérez de Acha, G. (2016). *Hacking Team malware para la vigilancia en América Latina*. Disponible en https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf.

Privacy International. (2018). Newly Disclosed Documents on the Five Eyes Alliance and What They Tell Us about Intelligence-Sharing Agreements. Disponible en https://privacyinternational.org/long-read/1998/newly-disclosed-documents-five-eyes-alliance-and-what-they-tell-us-about.

Sequera, M., Toledo, A. y Ucciferri, L. (2018). Derechos humanos y seguridad digital: una pareja perfecta. Disponible en https://web.karisma.org.co/derechos-humanos-y-seguridad-digital-una-pareja-perfecta/.

Unión Internacional de Telecomunicaciones (2014). *Entender el ciberdelito: fenómenos, retos y respuesta legal*. Disponible en https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_S.pdf.




Fundación
Karisma
@Karisma
@fundacionkarismaa
@karismacol
karisma.org.co
2020